



European  
Commission

# JRC TECHNICAL REPORT

## *Guideline* Building perimeter protection

*Design recommendations  
for enhanced security  
against terrorist attacks*

Karlos, Vasilis  
Larcher, Martin

2020



Joint  
Research  
Centre

EUR 30346 EN

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

#### Contact information

Name: Vasilis Karlos  
Address: via E.Fermi 2749, Ispra (VA), Italy  
Email: [vasileios.karlos@ec.europa.eu](mailto:vasileios.karlos@ec.europa.eu)  
Tel.: +390332789563

#### JRC Science Hub

<https://ec.europa.eu/jrc>

JRC 121582

EUR 30346 EN

PDF ISBN 978-92-76-21443-4 ISSN 1831-9424 doi:10.2760/20368

Luxembourg: Publications Office of the European Union, 2020

© European Union, 2020



The reuse policy of the European Commission is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated. For any use or reproduction of photos or other material that is not owned by the EU, permission must be sought directly from the copyright holders.

All content © European Union, 2020, except: *[cover page, N. Santoianni, image 1], 2020, Source: [Unsplash.com], [page 50, FEMA, image 28]*

For any use or reproduction of photos or other material that is not under the EU copyright, permission must be sought directly from the copyright holders.

How to cite this report: Karlos V., Larcher M., Guideline: Building Perimeter Protection: Design recommendations for enhanced security against terrorist attacks, EUR 30346 EN, European Commission, Ispra, Italy, 2020, ISBN 978-92-76-21443-4, doi:10.2760/20368, JRC121582.

# Contents

- Abstract..... 4
- 1 Introduction..... 5
- 2 Terrorism risk assessment ..... 6
  - 2.1 General..... 6
  - 2.2 Lessons learned from prior terrorist attacks ..... 8
  - 2.3 Risk assessment process ..... 10
    - 2.3.1 Threat identification..... 10
      - 2.3.1.1 Threat identification on national level ..... 11
      - 2.3.1.2 Threat identification on local level ..... 12
    - 2.3.2 Risk analysis ..... 12
      - 2.3.2.1 Exposed asset identification ..... 13
      - 2.3.2.2 Vulnerability identification ..... 14
      - 2.3.2.3 Likelihood and consequences assessment..... 14
    - 2.3.3 Risk evaluation ..... 17
  - 2.4 Key messages and challenges ..... 18
- 3 Protection against attacks with the use of explosives..... 20
  - 3.1 General..... 20
  - 3.2 Identifying worst-case scenarios..... 21
  - 3.3 Explosive materials ..... 23
  - 3.4 Loading definition ..... 25
  - 3.5 Blast wave parameters ..... 26
  - 3.6 Scaling laws ..... 27
  - 3.7 Calculation of blast loads..... 27
    - 3.7.1 Free-air bursts ..... 27
    - 3.7.2 Surface bursts ..... 30
    - 3.7.3 Air bursts..... 32
    - 3.7.4 Effect of angle of incidence ..... 34
    - 3.7.5 Clearing effects..... 35
    - 3.7.6 Damage definition..... 36
  - 3.8 Protective measures against explosive loads ..... 39
    - 3.8.1 Façade protection ..... 39
      - 3.8.1.1 Anti-shatter films (ASF) ..... 41
      - 3.8.1.2 Laminated glass ..... 42
      - 3.8.1.3 Catching systems ..... 44
      - 3.8.1.4 Supporting walls ..... 45

3.8.1.5	Contact detonations .....	45
3.8.2	Access control zones .....	46
3.8.2.1	Separation protective walls .....	46
3.8.2.2	Explosion venting .....	48
3.8.3	Protection against progressive collapse .....	50
3.9	Summary of blast protection design .....	55
4	Protection against attacks with the use of vehicles .....	56
4.1	General.....	56
4.2	Site survey.....	57
4.3	Attack scenarios.....	57
4.3.1	Vehicle size .....	58
4.3.2	Vehicle speed .....	59
4.4	Vehicle barrier types .....	60
4.4.1	Passive barriers.....	61
4.4.2	Active barriers .....	63
4.4.3	Innovative barriers .....	65
4.5	Barrier certification.....	65
5	Protection against unauthorised entry and ballistic attacks .....	71
5.1	General.....	71
5.2	Physical protection measures .....	71
5.3	Video surveillance .....	72
5.4	Access control and intrusion detection systems .....	74
5.5	CBRN-E sensors .....	75
5.6	Audio monitoring .....	76
5.7	Integrated systems .....	76
6	Protection against the malicious use of unmanned aircraft systems .....	78
6.1	Introduction.....	78
6.2	UAS categories .....	78
6.3	UAS threats against buildings .....	79
6.4	Countermeasures .....	80
6.5	Specific protection measures for buildings.....	83
6.6	C-UAS integration into the urban environment.....	84
6.7	Threats from other types of unmanned vehicles .....	85
7	Concluding remarks.....	86
	References.....	88
	List of abbreviations and definitions .....	92
	List of figures .....	93

List of tables ..... 95

## **Abstract**

The purpose of the current document is to provide guidance to security and law enforcement officials, building/site owners, venue organizers, state organizations, engineers and other stakeholders that are in charge of securing facilities and critical infrastructures against the growing international terrorist threat. The focus of the report narrows down into recommendations for a robust and usable approach for the physical protection of infrastructures against this borderless phenomenon. It addresses shortcomings encountered in the design of such security solutions and aims at producing a simple, self-contained practical guide to enable the selection and installation of elements that are able to stop and/or deter potential terrorist attacks.

A detailed analytical procedure is illustrated for identifying the weaknesses of potential terrorist targets and assess the relevant risk for different terrorist tactics. Advice is provided for the introduction of protection measures against both external and internal explosions and design methodologies are presented for minimizing the likelihood for the development of a progressive collapse mechanism. Moreover, specialized perimeter physical protection measures are proposed that may successfully restrict unauthorised vehicle and intruder access, supplemented by the employment of modern digital technologies, such as video surveillance, smart sensors and video analytics. The novel and emerging threat landscape is also addressed, such as the malicious use of Unmanned Aircraft Systems, requiring new response strategies that call for the adoption of state-of-the-art counter technologies.

# 1 Introduction

The guidance drafted at the current document provides a methodology for securing buildings against intruders, terrorists and other physical threats that try to intrude or gain access to a vulnerable asset. The focus is on the introduction of concepts that are applicable to the design of building security and aim in protecting people and property by enforcing a security perimeter. An asset's secured perimeter can be considered as the first line of defence in a multi-layered protection scheme.

More specifically, the first chapter of the document is dedicated to providing a robust and usable risk assessment process against terrorist threats. The proposed assessment approach is focused on buildings and other built facilities that are considered the exposed asset and classify them in terms of potential impact and probability of occurrence. The threat of terrorism is characterized by great uncertainties, so a full quantitative assessment is impossible. Nevertheless, a first step is attempted in providing a semi-quantitative method, which in combination with qualitative parts, may decrease the subjectivity of a risk analysis based solely on expert judgement.

The next chapter contains general principles and recommendations concerning the application of external blast actions on structures and structural components and should be used in conjunction with the Eurocodes [EN1990, 2005] and [EN1991, 2001]. The provided load parameters are valid for close-in, intermediate-range and far-range detonations. Explosions are extremely complex phenomena and are characterized by a great number of uncertainties concerning the type, location and mass of the explosive device, the blast parameters, the environmental conditions etc. Blast-resistant and protective design focus on techniques for limiting and mitigating the damage after an explosive attack and increasing the chances of survival of the occupants. The structure or structural component under attack should still be able to fulfil their original design purpose, as with the applied design approaches the loading is reduced to acceptable levels. For adopting these design approaches, the calculation of the blast loading parameters to be inserted in the analysis is a prerequisite. Since a procedure for estimating these parameters is missing in the Eurocodes, the recommendations that comprise the current guide attempt to fill this gap, along with suggestions on mitigation measures.

Subsequently, advice regarding the protection from attacks that use vehicles to breach the security perimeter of a facility is provided. A growing number of vehicle ramming attacks have been recorded in the last years, showing a tendency in using vehicles as a weapon to target the public or gaining access to sensitive facilities. The popularity of such attacks is attributed to their easy planning, the direct accessibility to a variety of vehicles and the minimal required expertise. A structured approach is proposed in selecting, installing and using vehicle protective security barriers, that guarantees the adoption of tailor-made measures instead of 'one-size-fits-all' solutions.

A chapter also sheds light to key issues and possibilities that are provided by the proliferation of new digital technologies. A synthesis of the most recent and efficient digital security systems that can be integrated to setting up and maintaining a building security perimeter is provided. The decisive role of the installed software in taking full advantage of the capabilities of the installed system is underlined, as well as the challenges faced in the harmonic cooperation when multiple security systems are employed.

The last chapter is dedicated to the malicious use of Unmanned Aircraft Systems (UAS), a relatively new security threat for sensitive buildings. Weaponised UAS have already been used by terrorist groups outside Europe and there is a rising concern that similar tactics may be used for targeting infrastructures and public events. This risk becomes greater as the number, payload, operating range and speed of commercially available UAS is rapidly increasing, while their cost is decreasing. Up to now protecting a sensitive building from a terrorist attack or other forms of intrusion, comprised of setting up a physical security perimeter, access control systems and adopt an engineering design capable of mitigating mainly ground attacks. The fast increase of the worldwide number of UAS and their simple and remote piloting capabilities clearly demonstrates the need to be considered during the establishment of a holistic building security scheme.

## 2 Terrorism risk assessment

### 2.1 General

Over the last years, the fear of terrorism is steadily one of the main concerns of Europeans, as can be witnessed by the latest Eurobarometer surveys (Standard Eurobarometer 92, 2019). This is mainly attributed to its unique characteristics, unpredictable nature and the extensive coverage of attack incidents by the media. Even though terrorist events are of low frequency, a comprehensive understanding of the parameters that influence their likelihood is required for establishing a robust risk assessment and management framework. Independent of their rarity, their psychological, economic and political impact on society can be disproportionately high, as demonstrated for example after the bombing attacks in Brussels and the vehicle-ramming attack in Nice in 2016. As a result, the European Commission has issued an 'Action Plan to support the Protection of Public Spaces' (European Commission, 2017a) that Member States, regions and cities are advised to incorporate into their infrastructure development program.

As mentioned in the Commission Staff Working Document (European Commission, 2017b) developed through the results of the National Risk Assessments (NRAs) of Member States, the global terror threat is uncertain due to its complex and fragmented nature, that includes both structured groups and individual (lone wolves) aggressors. In particular, scenarios concerning individual terrorist actions aiming public spaces and critical infrastructures have been developed with links to political and religious extremism. A terrorist attack could potentially have cascading effects and cross-sectorial consequences, e.g. large-scale contamination after an attack with a toxic agent or environmental disaster after a substance release.

Terrorist events can be defined as intentional violent acts performed under the pretext of political, religious or social motives, whereas crime is usually driven by economic or retaliation intentions. The borderline between terrorism and military conflicts (encounters in which armed combat among military forces takes place either at international or national level) might be hard to be distinguished, since both rely on the extensive use of violence and could be guided by similar motives. Weapons (firearms, knives etc.), vehicles, CBRN (Chemical, Biological, Radiological and Nuclear) devices and improvised explosive devices (IEDs) that are either homemade or purchased in the black market are the preferred attack methods of terrorist groups and lone actors. However, it is important to consider that the modus operandi of the aggressors (in both terrorist acts and military conflicts) can rapidly transform, as has been demonstrated in the recent past. This transformation depends on a number of factors, such as the current political, economic and religious status that are driving the motives, the skills and capabilities of the perpetrators, the availability of financial and human resources, the instructions and guidance available in terrorist propaganda sites and magazines.

The risk of terrorism exists in both developed and developing countries and it still poses a major concern in certain regions that are mainly located in Africa, the Middle East and Asia, as shown in Fig. 1. Nevertheless, the recent attacks in the Western world have clearly demonstrated that terrorism is a worldwide phenomenon, featuring complex direct (e.g. victims, injuries, loss of property) and indirect (e.g. psychological) consequences on the society. Unfortunately, the unique characteristics of terrorism risk are often neglected, resulting in a lack of dedicated guidance material for assessing and managing the relevant risk. Therefore, the establishment of a national terrorism risk assessment plan is crucial for identifying critical zones, popular tactics and get the overall picture regarding the economic, social and political consequences in case of a successful attack.



**Figure 1.** Global terrorism threat level in 12/2019-05/2020 by JRC terrorism database using EMM. (Background map © Mapbox, © OpenStreetMap).



The varied, cross-border and cross-sectorial nature of terrorist attacks is addressed at the EU level in the European Agenda on Security (European Commission, 2015) and the Security Union Strategy (European Commission, 2020), which aims at assisting Member States in ensuring security through coordinated and effective response at the European level. As a result, several operational measures have been proposed to significantly reduce the number of inherent vulnerabilities that were exposed in previous terrorist attacks and enhance the overall security of potential targets.

The development of a risk assessment and risk management procedure in the field of terrorism is an overwhelming task and presents a challenge for every Member State, local authority and private stakeholder in terms of complexity, time and resources. Providing answers to terrorism-related issues (e.g. how to prioritize the assets to be protected, how to strike the right balance between effective and cost-efficient countermeasures) is more difficult than the ones concerning natural hazards, since terrorist attacks are intentional, driven by different motives, and the relevant risk incorporates numerous attack scenarios (e.g. blast, vehicle, UAS, active-shooter, knives), resulting in approaches that may differ greatly depending on both the examined asset and the attack type. Risk assessment aims at estimating the potential impacts of terrorist acts, their severity and their probability of occurrence. As different assets require very different analysis of their risk, questions usually arise concerning how to establish a terrorism risk management plan, how to initiate a terrorism risk assessment process, what are the best mitigation/deterrence strategies and how to prioritize the allocation of resources. As has already been demonstrated in the management strategies of other risks (e.g. drought, earthquakes, floods, biological disasters, chemical and nuclear accidents), the proposed scheme should incorporate an orderly approach for identifying and tackling the threat of terrorism.

In the current chapter, the definition of risk assessment according to the ISO 31010 (ISO, 2018) will be employed, even though the steps that are described in the standard concerning the risk assessment process are generic so as to cover both natural and human-induced hazards. Certain shortcomings in the risk assessment methodology have already been pointed out by preceding documents (ISO 31000:2009), such as the difficulties in estimating the likelihood of rare events and the quantification of consequences in the human/social domain. Several different terrorism risk assessment methodologies exist, which are usually shaped from the interested stakeholders to satisfy their unique needs, leading to non-uniform practices. The approach that is proposed herein, is based both on the provisions of ISO and a collection of best practices related to the risk assessment of various hazards/threats, introducing techniques that can assist stakeholders

in assessing the risk of their asset regarding terrorist attacks. It focuses mainly on the threats targeting infrastructures and public spaces and starts with identifying the prevailing attack modus operandi at a national/local level. Subsequently, continues with the analysis of the risk for the examined asset, concentrating on its vulnerabilities, importance and potential impact should an attack materialize. Finally, the risk is evaluated and is termed as either acceptable (no measures need to be taken), or unacceptable (appropriate mitigation measures need to be taken). The chapter also tries to shed light on the substantial gaps and challenges that generate obstacles in the calculation of the risk from terrorist attacks.

## 2.2 Lessons learned from prior terrorist attacks

The deadliest terrorist attacks have been usually carefully planned (or at least to a certain degree) to maximize the number of casualties, increase the generated damage and draw the attention of the media. Targets are usually selected according to their vulnerability and past experience has shown that unprotected sites have higher chances of being attacked. Predicting locations and type of a potential attack is a challenging task, since there exist many different factors that affect the reaction of the aggressors. In this section, a selection of indicative cases of terrorism incidents, which resulted in a large number of victims and injuries, is presented, emphasizing on their common characteristics and underlining the lessons-learned that have influenced the selection of protection measures against terrorism acts, serving as useful examples for future risk assessments.

- One of the most notorious terrorist acts resulting in a great death toll is the attack against the World Trade Centre in New York, USA on 11<sup>th</sup> September 2001, which took place in parallel to other attacks in the USA. The attack included sophisticated and detailed planning, aiming at structures of symbolic value, while guaranteeing a great number of victims and provoking panic and fear to the population. The use of asymmetric warfare techniques led to the realization that both public spaces and critical infrastructures could be potential targets of terrorist attacks and that different strategies need to be adopted for resisting the aggressors. The business and economic activities at the affected sites were disrupted for many weeks due to the widespread destruction causing severe consequences at the financial sector and air traffic. The 19 terrorists who hijacked four airplanes, were members of the Al-Qaeda network and four of them had received specific pilot training in the USA without raising suspicion to the secret services.
- On 19th April 1995 in Oklahoma City, USA a vehicle borne explosive device (equivalent to approximately 1800kg of TNT) was detonated in front of the A. P. Murrah building resulting in the collapse of approximately one third of the structure. The attack was performed by two US citizens that had undergone military training, though not belonging to a terrorist group, and was extensively planned. It targeted a structure that housed several state facilities, as the aggressors wanted to disapprove several governmental actions. Bomb ingredients were acquired from local stores and the bomb was placed in a rental truck that was parked on the sidewalk outside the nine-storey building. After the attack, the remaining standing structure was demolished due to safety reasons and several years were required for constructing a new facility that substituted the old one.
- On 13th November 2015, Paris experienced a series of coordinated terrorist attacks that resulted in a great number of victims and injuries. The aggressors used person-borne improvised explosive devices (suicide bombers) and assault rifles attacking a sport stadium, a music theatre and several restaurants and bars. The perpetrators belonged to the ISIL group and claimed that the motives behind the attacks were the ideological objections to the western lifestyle. Clearly, the simultaneous attacks against multiple targets, reveal the existence of a sophisticated plan against places of mass congregation that maximized the number of victims and drew the attention of the media.
- One of the deadliest vehicle-ramming attacks took place at the city of Nice against the thousands of people gathered at the city's waterfront during the Bastille Day celebrations. On 14th July 2016 a 20-ton rented cargo truck attacked the public by managing to attain a speed of 70-80km/h, as the road leading to the pedestrian zone was an almost straight path. Because of its mass and speed, the truck managed to force its way through the existing light protection measures (crowd control portable barriers, lane dividers etc.) and covered a total distance of approximately 1.7km before being stopped by the police. In order to increase the number of victims, the terrorist, who had not been involved in major crimes before, was driving the truck in a zigzag fashion boarding the crowded sidewalks whenever possible. Police investigation revealed that the aggressor had been planning the attack for over a year and that he had surveyed the site while driving the rented truck on numerous occasions before the assault date. He was born in Tunisia and had been living in France for more than 10 years,

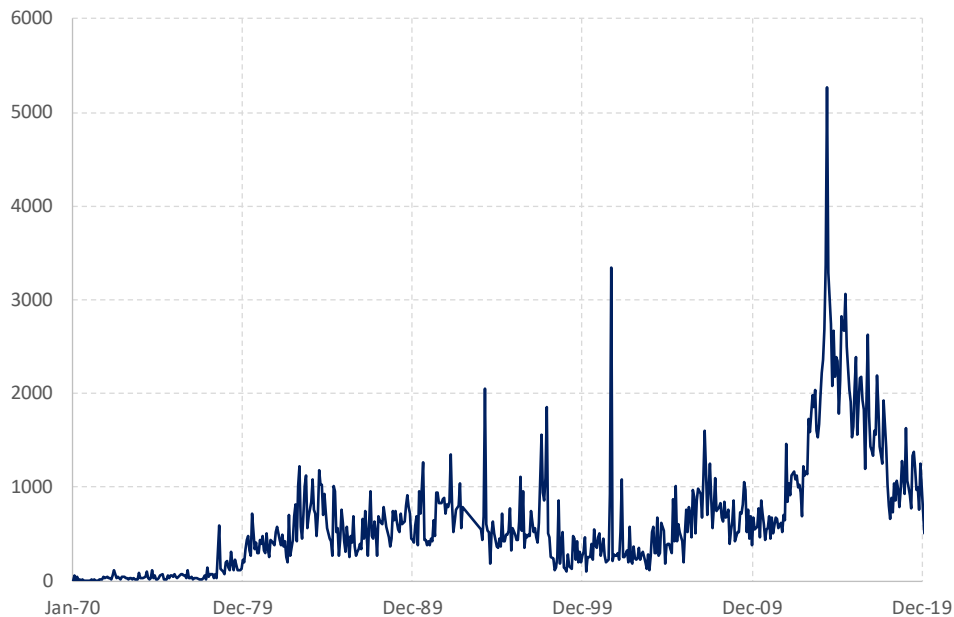
while he had been previously involved in minor crimes and was radicalized, sharing the views of the Islamic State, shortly before the vehicle-ramming incident.

The above-mentioned events are only a small fraction of the number of terrorist attacks that have been performed over the last years and constitute an indicative sample of different scenarios (including the use of airplanes, explosives, weapons and vehicles as the preferred attack methodology) that shares a substantial number of characteristics. It is clear that the majority of the described incidents were carefully planned in advance, as the aggressors had examined the attack sites beforehand to mark their vulnerabilities. The targets were iconic structures and places of mass congregation that would cause mass casualties, gain media attention and spread terror and fear at the population. The sites were characterized by the absence of (or the presence of insufficient) protective measures that would be able to deter or mitigate the consequences of the assaults. The outcome of the attacks resulted in a great number of victims, damages on infrastructures, economic losses that lasted for a long period and psychological impacts on the society. The majority of the aggressors were not considered a threat by the local intelligence agencies, even though many of them had adopted violent extremism after being inspired from radicalised preachers and online propaganda (especially for Jihadist related attacks).

It is highlighted that aggressor tactics and targets may quickly change introducing attack techniques that were not considered before, as happened during the 9/11 attacks. For instance, Radiological Dispersion Devices (RDD's, also known as "dirty bombs") might be used by terrorist groups as they can be constructed by combining conventional explosives with radioactive material normally used in nuclear medicine and industrial applications. Growing security concerns also exist regarding the use of Unmanned Aircraft Systems (commonly referred to as drones), whose technology has proliferated in the last years and have already been used for terrorist attacks outside Europe.

However, not all terrorist attacks are extensively planned and may be of opportunistic character resulting in lighter consequences. The impact of an attack on the society is not necessarily only related to the number of fatalities and injuries, as even failed attacks may have significant psychological implications to the public. Depending on the information source, the worldwide number of terrorist attacks in the last years is approximately 20,000 per year and the number of yearly casualties about 25,000.

**Figure 2.** Fatalities per month from Global Terrorism Database (1970-2017, year 1994 is missing in the recordings) and Control Risks (2018-2019).



## 2.3 Risk assessment process

ISO 31010 provides a generic approach to managing various risk types, since it is not directly correlated to a specific hazard or asset, while EN 1991-1-7 (EN 1991-1-7, 2006) provides a risk assessment process against accidental loads in the field of buildings and civil engineering structures. The most common approach for assessing the risk of a certain site can be divided in three distinct steps that can help decision-makers in prioritizing their security needs: risk identification, risk analysis and risk evaluation. If the risk assessment process within a terrorism context follows the same format, it could be categorized into the following stages:

- **Identification** of potential terrorist threats by gathering all available information on the risk components and development of relevant attack scenarios.
- **Risk analysis** (qualitative, semi-quantitative or quantitative) to estimate the likelihood of occurrence and the potential consequences for the exposed assets, while taking into account the vulnerabilities of each potential target.
- **Evaluation of the relevant risks** for each attack scenario and asset in order to decide whether further action is required, and which is the best tailor-made strategy for reducing the risk to an acceptable level.

The risk assessment concerning terrorist threats can be performed at various levels, depending on the asset that is examined. It may be performed at the local level if a stand-alone, specific asset is considered or at a city, regional or national level if a whole sector is analysed. The decision for initiating a risk assessment lies in the hands of the relevant stakeholders (building/site owners, venue organizers, state organizations, security and/or law enforcement officials etc.) and their engagement is crucial for tackling the far-reaching consequences of a potential attack. Clearly, the analysis results may differ substantially depending on the stakeholder performing the risk assessment, as their views on risk may differentiate depending on their experience and goals.

**Figure 3.** Risk assessment process.



### 2.3.1 Threat identification

The first step in the risk assessment process is the identification of potential terrorist threats that are relevant for the region and the target under consideration. Threat identification focuses on pinpointing potential terrorist tactics and providing the framework for determining effective prevention and/or mitigation measures. For estimating the likelihood of occurrence of a terrorist attack and formulate potential attack scenarios, one has to resort to available statistical data from recent incidents and investigate information that is available from

counterterrorism units, intelligence services, state and emergency agencies and the internet. Attack scenarios should be rated according to their feasibility and probability. For example, the probability of vehicle ramming incidents is usually higher compared to attacks with the use of explosives due to the terrorists' direct accessibility to a variety of vehicles, the minimal required expertise and the easy planning. In general, during assessing terrorist threats, decision makers and assessors tend to put more emphasis on past events failing to "think the unthinkable". New tactics may emerge that, even though they might be characterized by a smaller probability, could result in higher societal, economic or political impact. A scenario-based approach at potential targets is bound to simplify the complexity of the risk assessment process and assist in the evaluation of the different targets in terms of criticality (i.e. consequences severity).

**2.3.1.1 Threat identification on national level**

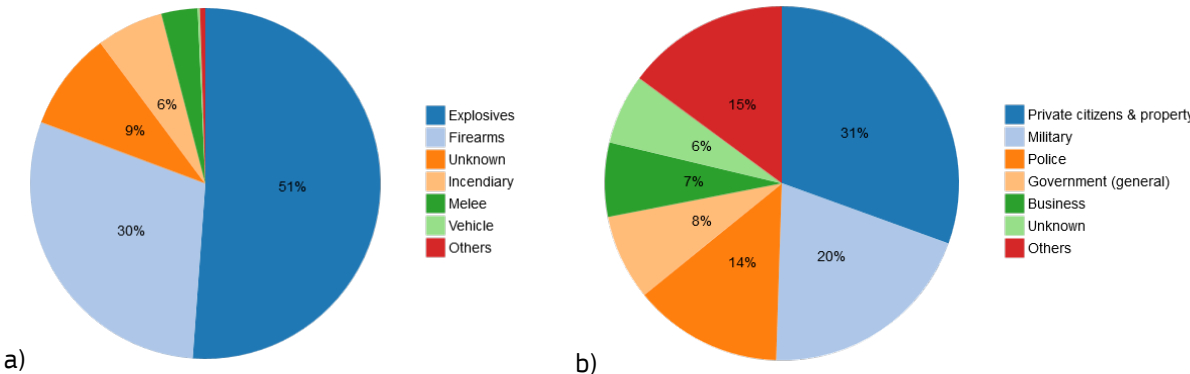
The nature of extreme manmade events with malicious intent, such as terrorist attacks, differentiates them from other natural hazards. Their intentional character means that they are not as common as, for example small scale earthquakes, floods or droughts. Classical statistical approaches may provide an indication for calculating future risk, even if in some cases the statistical basis might not be wide enough. Detailed data from additional sources, such as intelligence agencies, could be required for a more rigorous analysis. Information included in propaganda sites and magazines can greatly contribute in identifying potential attack scenarios against specific targets. Nevertheless, information concerning potential terrorist threats is not always readily available due to its sensitive nature and access may be granted only to authorized individuals and not to private stakeholders. Moreover, the risk needs to be re-assessed in regular intervals to analyse any new security-related information and relevant threats, especially since a major part of malicious events is politically or religiously motivated and can rapidly transform, as has been demonstrated in the recent past.

Potential attack scenarios can be estimated by examining any observed criminal activity in the area of interest and possible recorded incidents or security breaches over a certain time period. Possible data sources are:

- Global terrorism database (University of Maryland, 2018), which is freely available but updated on an annual basis, which means that latest data are not readily available.
- Commercial security risk providers like Jane's (IHS Markit, 2019) or Control Risks (Control Risks Group Holdings Ltd, 2019) databases.
- European Media Monitor (European Commission-EMM, 2020) system that analyses information from both traditional and social media. The usability of the provided data to create a terrorism tool by using machine learning approaches is currently tested by the JRC. A first result of that approach is shown in Fig. 5.

Since terrorism threats can completely change over time, special attention should be paid on very recent events, thus it is advised that higher statistical weighing factors are assigned to such events during the threat identification process compared to older ones. Supporting information that can prove valuable during this threat identification process may be located in organized crime databases, such as the number of firearms in circulation, the terrorism funds obtained via drug trafficking etc. For example, the pie charts presented in Fig. 4 highlight the worldwide predominant assault types and targets over a four-year period (2014-2017).

**Figure 4.** Worldwide terrorist attacks by a) utilized modus operandi and b) target.



Assessing the risk of terrorism on a country level, can prove useful in identifying critical countries, yet the results are usually too general for recommending and implementing specific actions. A breakdown of risk to smaller regions is even more questionable, since the statistical significance of available data might not be adequate for performing a reliable assessment. The development of worldwide critical terrorism-affected zone maps (e.g. Niger, Afghanistan, Yemen) that demonstrate terrorist incidents, like the one presented in Fig. 5, can assist in classifying hot spots and issuing travel advices, but are impractical if the introduction of specialized protective plans is of interest.

**Figure 5.** Threat level from terrorist attacks in central Africa and Middle East in 12/2019-03/2020 by JRC terrorism database using EMM. (Background map © Mapbox, © OpenStreetMap)



**2.3.1.2 Threat identification on local level**

Carrying out a threat identification on a local level is a challenging process, as a definite “yes or no” answer concerning imminent attack types cannot be provided. Quantifying the probability of a terrorist attack against a specific target may seem futile, as by nature it contains many uncertainties. Examining statistical data from previous similar events at the region and potential target of interest using the databases that have been described in the previous section, can provide valuable indications concerning its threat rating. Nevertheless, usually there are not adequate data (especially in Europe) to support the assessment and expert judgement is required to identify the specific threats that are of interest to the examined asset.

**2.3.2 Risk analysis**

To determine the risk level, a dedicated risk analysis has to be performed, where the various risk components and drivers are combined, such as the specific threat, the exposure (including attendance) and the asset’s vulnerabilities. Each risk analysis may greatly vary in degree of detail as it depends on the availability of data and the way the uncertainties and vulnerabilities are addressed. The risk analysis needs to provide the likelihood of an attack and the consequences, should such an attack materialize. Within this process the assets that are exposed to such an attack need to be identified, pinpointing their vulnerabilities and evaluating their influence on the probability of an attack.

### 2.3.2.1 Exposed asset identification

A crucial step in the risk assessment process is the identification of the assets that have to be considered in the analysis, if they have not been expressly preselected by the relevant stakeholder. Recent terrorist attacks have shown that there is a recurrent targeting of unprotected public spaces of mass congregation of various gathering purpose, as shown in Table 1. These are also known as soft targets, meaning targets characterized with high concentration of people and absence of specific security measures. They are the opposite of “hard targets” that indicate grounds equipped with heightened protection and surveillance. Target attractiveness depends on many different factors that are associated with both the terrorist group and its motivation, and the characteristics of the target. For instance, aggressors may choose a target that is against their political, social or religious ideology, while the selection may be also influenced by the availability of funds and the size of the terrorist group. This means that religious or cultural symbols that are considered to be promoting the Western lifestyle, capitalism and/or democracy may become the target of Jihadist terrorists, while governmental facilities and minority establishments may seem attractive to right-wing terrorists. Iconic and recognizable locations have higher chances of being attacked, especially if they are mentioned in terrorist propaganda magazines. Popular tourist locations, open-air festivals, sport events, landmarks and areas that are typically characterized with high people presence and lack of security guards are also appealing to terrorists.

**Table 1.** Soft target categories.



Target category	Examples of infrastructures	Occupancy level
<b>Recreational</b>	Stadiums, concert halls, entertainment venues, festivals, parks, markets, shopping malls, theatres, cinemas, clubs, restaurants, bars, cultural events, parades, pedestrian areas	High
<b>Industrial</b>	Factories (electricity, nuclear, chemical, plants etc.), refineries, warehouses	Low-medium
<b>Commercial</b>	Hotels, apartment buildings, office complexes, shops	Medium
<b>Governmental</b>	Police stations, barracks, town halls, courts, prisons, fire stations, official residences	Low-medium
<b>Religious</b>	Churches, religious events, places of worship	
<b>Political</b>	Embassies, landmarks, tourist monuments	Low
<b>Public</b>	Hospitals, medical centres, universities, schools, museums, libraries	High
<b>Transportation</b>	Train and subway stations, airports, bus and port terminals, transportations sites	Low

The weighing factors for evaluating the criticality of each exposed target may be different among the various countries, but some common indicators (e.g. people attendance, site symbolism, facility size and importance) may be used for identifying the sites where the potential consequences have the greatest impact. Such a process guarantees improved, custom-made security and mitigation actions, though differences may appear depending on the stakeholder responsible for performing the identification. For instance, the criticality of a certain target from the building/site owners’ perspective is usually related to its operation, whereas state organizations and policymakers may be more attentive to the public’s security and needs. Consequently, during the design of an effective physical security strategy the harmonic collaboration of all relevant stakeholders is crucial for effectively tackling the interdependencies between the different assets.

### **2.3.2.2 Vulnerability identification**

Vulnerabilities are the inherent weaknesses of a potential target that may render it susceptible to the destructive consequences of a terrorist attack and greatly affect its risk level. These vulnerabilities can be exploited by perpetrators in their effort to strike. Thus, effective mitigation measures and identification of optimal strategies are required for minimizing exposure and enhancing resilience. A detailed examination of the asset under consideration can disclose deficiencies and flaws that may encourage the formulation of an attack plan, as, for instance, the lighter the security measures, the more attractive a target is deemed to the eyes of terrorists. An objective assessment of the vulnerability degree of a public space or infrastructure is a challenging task, as there are many different factors that should be taken into account, such as the target's accessibility, its significance, its location, its shape and protective measures that may be present (entry checks, video surveillance, security guards, perimeter protection etc.). DG HOME has developed a vulnerability assessment checklist that considers the following attack modes:

- Firearms – Small calibre pistols or semi/fully automatic rifles
- Bladed Weapon – Knives, machete or other sharp and blunt objects
- Vehicle Ramming – Use of vehicle for ramming crowded places
- Improvised Explosive Devices (IED) – Carried or concealed in objects or goods
- Person Borne Improvised Explosive Devices – Concealed on a person
- Vehicle Borne Improvised Explosive Devices – Concealed inside a vehicle
- Unmanned Aircraft Systems (UAS) as a weapon and UAS borne IED or agents (CBRN-E)
- Biological Agent – Concealed in goods or carried items
- Radiological Agent – Concealed in goods or carried items

Even though these threats are unlikely to take place simultaneously, they emphasize the complexity and plethora of different attack scenarios. A site's vulnerabilities need to be combined with people attendance so as to arrive in a preliminary evaluation of the potential target's risk level. An example of a vulnerability assessment categorization is shown accordingly:

**Low vulnerability:** The examined asset (infrastructure or public space) is equipped with adequate security countermeasures (controlled access, safeguards, perimeter protection etc.) to drive away potential aggressors and is unattractive as a potential target.

**Moderate vulnerability:** The examined asset (infrastructure or public space) may be equipped with some security countermeasures (no controlled access, some safeguards, partial perimeter protection etc.) and is well-known only at a local scale.

**High vulnerability:** The examined asset (infrastructure or public space) is characterized by inadequate security countermeasures, while it is well-known at a national scale.

**Very high vulnerability:** The examined asset (infrastructure or public space) is characterized by inadequate security countermeasures, while it is well-known at a global scale.

### **2.3.2.3 Likelihood and consequences assessment**

The introduction of a universally applicable method for calculating the likelihood of a specific attack type against a certain target is problematic due to the frequently opportunistic character of attack planning and the absence of sufficient data. Moreover, due to the nature of the terrorist threat, the majority of the required information is possessed by various intelligence services and is of restricted nature, which makes the assessment of the probability of an attack a challenging task. Despite the fact that no concrete conclusions can be drawn from analysing the potential modus operandi of the aggressors (attack scenarios), some valuable information regarding the likelihood of an attack can be deduced by responding to several questions that may arise during the assessment process including, but not limited to:

- Are there any indications of an imminent terrorist attack at a local, regional, national or international level?
- Does the potential target represent a religious/ethno-nationalist ideology that is against the political or religious agendas of active terrorist groups?
- Is the target of symbolic or historical value?
- Which is the maximum attendance?



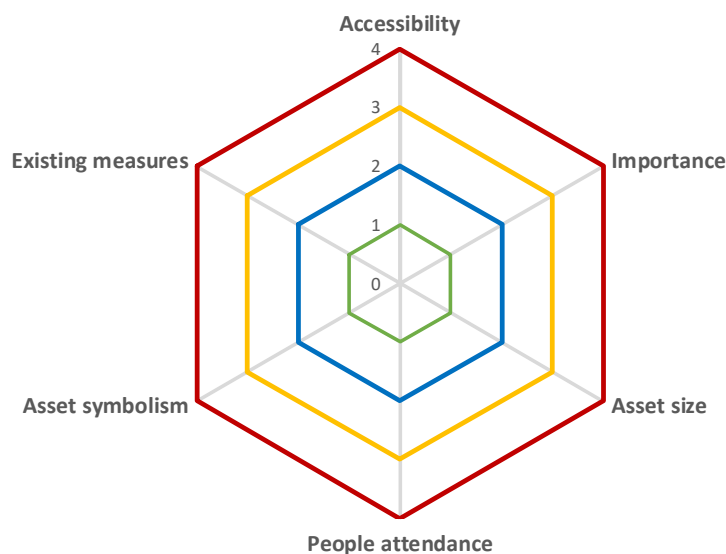
- Are there any high-profile events hosted that are attended by famous people and covered by the media?
- Are there any trained security officials present?
- Are there any security measures already deployed (access control, CCTV, security barriers, perimeter protection, UAS countermeasures etc.)?
- How easily accessible are the target's premises and by what means (vehicles, motorcycles, on foot etc.)?

To provide a certain value on the criticality of an asset/building structure and the likelihood of an attack, a number of indicators may be used, similar to the approach proposed by the US Interagency Security Committee (ISC, 2013). According to this method, a point system is introduced that may be used to provide an estimate of the facility's criticality. Herein, six different factors with equal weights are evaluated and after their scores are summated, the examined asset/site is categorized according to its criticality. The main characteristics of each indicator are:

- **Accessibility:** Is a measure of the openness of the examined asset to the public, of any reported previous threats (to the asset or the users) and the crime rate at the surrounding area.
- **Importance:** Depends on the asset's tasks, its interdependencies with other facilities and the consequences to the state and the society after a potential attack.
- **Asset size:** Demonstrates the space (in square meters) that is occupied by the asset.
- **People attendance:** Shows the maximum number of people (personnel and visitors) that are present in the asset during peak hours.
- **Asset symbolism:** Is linked to the attractiveness of an asset as a potential target and the probability of being considered to be promoting a lifestyle that is against the political, social or religious ideology of aggressors. It also includes popular tourist locations, landmarks and cultural sites.
- **Existing measures:** Considers security measures that are already present in the examined facility and may render it less attractive in the eyes of possible aggressors.

Fig. 6 presents the examined indicators and the points that have to be allocated (1 to 4) to each of them, while Table 2 shows in detail the scoring criteria to be followed when assigning the points. It is underlined that these scoring criteria do not cover all the different cases that may be used for characterizing the criticality of an asset. Thus, the scope of the current process is to provide a simplified process for conducting a preliminary assessment regarding an asset's criticality. If the characteristics of the examined facility satisfy more than one column per indicator in Table 2, the highest score has to be assigned per indicator when determining the criticality of the asset.

**Figure 6.** Indicator point system for assessing criticality of exposed assets.



**Table 2.** Scoring criteria per indicator.

	Allocated points	1	2	3	4
<b>Indicators</b>	<b>Accessibility</b>	-No public contact -No previous threats -Minor-crime area	-Little public contact -Some previous threats in the surrounding area -Low-crime area	-Normal public contact -Previous threats against the facility -Moderate-crime area	-High public contact -Usual presence of protests -Usual threats against the facility -High-crime area
	<b>Importance</b>	-Insignificant impact at national level in case of an incident -Activities only at local level	-Some impact at national level in case of an incident -Activities only at regional level	-Significant impact at national level in case of an incident -Activities at national level	-Very big impact at national level in case of an incident (e.g. critical infrastructure) -Activities at international level
	<b>Facility size (A)</b>	$A < 1000m^2$	$1000 < A < 10000m^2$	$10000 < A < 25000m^2$	$A > 25000m^2$
	<b>People attendance (N)</b>	$N < 100$	$101 < N < 250$	$251 < N < 750$	$N > 751$
	<b>Site symbolism</b>	-Not well-known facility	-Well-known at a local level -Symbolic only at a local level	-Well-known at a regional level -Symbolic only at a regional level	-Well-known at a national level -Symbolic at a national level (tourist attraction)
	<b>Existing measures</b>	-Elevated physical security measures -Presence of multiple security guards	-Some physical security measures -Presence of limited security guards	-Basic physical security measures -Absence of security guards	-Absence of physical security measures -Absence of security guards

After assigning the relevant points to the abovementioned indicators, the points are added together and the criticality of the asset may be defined, as shown in Table 3. The criticality level of an asset (low, medium, high or very high) is directly linked to the required protection level and the specific security measures (additional or not) that have to be adopted. The type of measures depends on the asset that has to be protected and need to be decided by both the stakeholders and experienced professionals, as will be discussed in the risk evaluation section. A facility may also be moved to another category after a careful consideration of indicators that were not taken into account.

**Table 3.** Assessment of an asset's criticality.

Asset criticality	LOW	MEDIUM	HIGH	VERY HIGH
Asset score (points sum)	6-9	10-15	16-21	22-24
Required protection level	LOW	MEDIUM	HIGH	VERY HIGH

The consequences of an attack are directly linked to the type of target selected by the terrorists and the conditions at the time of the assault. For instance, an attack against a city square will have a completely different aftermath if it is performed during peak hours or during social events when the crowd attendance is

at its highest. The impact of past attacks, such as the effects on human life (injuries, fatalities etc.) and the economy (repair cost, disruption of services etc.), can be used as input for assessing the repercussions of potential future events. Indirect consequences from a terrorist attack are more difficult to be assessed, as they include the social and (indirect) economic costs, such as the effects on the population's psychology and the impact on the tourism industry (Larcher, 2018). Cascading phenomena may also appear through the interconnections among infrastructure systems, such as for instance after a terrorist attack against a power plant which, apart from the immediate life losses, would also result in disruptions in many other sectors.

Consequence assessments serve as a tool for estimating the outcome of different attack scenarios at various sites and categorize them in terms of severity. However, many of the components of terrorist risk and their impact are not quantifiable (especially the ones related to the social and psychological consequences) and entail a very large degree of uncertainty. Since specialized quantitative approaches for measuring the consequences of an attack are still missing, qualitative methods and expert judgement may provide valuable insight at the dependencies among the different affected elements. Further details on indicators to be used for analysing the consequences from a terrorist attack can be found in the (Sendai Framework for Action on Disaster Risk Reduction 2015-2030).

**2.3.3 Risk evaluation**

During the risk evaluation stage, the results of the risk analysis are evaluated and an appropriate response is selected, indicating and prioritizing the attack scenarios that have an increased likelihood or greater consequences and should be tackled first. Different response alternatives have to be considered, depending on the desired outcome and the availability of resources. The risk can be either **deemed acceptable/tolerable**, so no further action is needed, or may be considered unacceptable, which means that an intervention is required, as shown in Fig. 7. The intervention can be performed by adopting measures that aim in **mitigating** the consequences and the probability of an attack (e.g. by limiting the access to explosive precursors and firearms or improving counter-intelligence units) or by adopting **hardening measures** that guarantee increased protection. The former approach translates into moderate cost and an intermediate risk reduction, while the latter offers greater risk reduction, but at a higher cost. Regardless of the preferred risk administration option and since 'zero risk' does not exist, the remaining accepted risk (even if no intervention is adopted) needs to be supported by a thorough action plan in case of an attack (e.g. management of first responders) and public awareness campaigns.

The criteria under which the risk is evaluated are based on a mixture of socio-economic-political factors, that can be very different among Member States, local authorities or private stakeholders. In other words, before arriving at a decision, certain components are considered, including the cost of an intervention, the existing legislation/codes, the presence of physical obstacles, the potential effects on the daily life of the public, the social perception and the political cost.

Figure 7. Risk administration options.



Decision makers, who are usually different from the expert group responsible for the risk analysis, are frequently required to make a 'judgement call' concerning the action that should be followed, due to the large degree of uncertainties a terrorist attack risk analysis entail. One of the main concerns during these evaluation procedures, is the definition of an acceptable risk level, since providing protection against all possible terrorist threats is not feasible in both economic and practical terms. Clearly, it is difficult to describe the severity of potential consequences by using a single parameter, as it is extremely challenging to assign a value on human life and compare it with lifeless objects. Nevertheless, the results of the risk analysis can provide useful information that can facilitate the employment of the most effective actions and the prioritization of the exposed assets in terms of criticality.

The task of deciding the specific action that needs to be undertaken requires close collaboration between the decision-makers, that evaluate whether the action is required, and experts, that can facilitate the selection of the most efficient solution. For instance, in case of the protection of the built infrastructure against explosive events, specialized engineers are required to intervene on the aspects of engineering design, such as:

- Resistance against progressive collapse. Increasing structural robustness by employing methodologies similar to the ones designed for resisting the effects of severe earthquakes.
- Resistance of glazing material. Increasing the performance of glass under blast loads. Its presence in nearly every building's façade and its extreme fragility creating glazed fragments is responsible for a large fraction of the injuries and fatalities during explosive events. The use of laminated glass panels or anti-shatter films guarantees a higher resistance to blast loads and reduces the relevant risk.
- Protection of soft targets/people. Decrease the mortality rate for the public by enforcing a stand-off perimeter through the introduction of a combination of tailor-made active (access control, security guards, video surveillance etc.) and passive (stiff protective elements and barriers that are harmonically integrated into the surrounding urban environment) protection measures.

## **2.4 Key messages and challenges**

Given the diverse targets and tactics selected by terrorists in their effort to cause victims and draw public attention, a multidimensional response is needed, one that includes innovative new approaches in the assessment of the relevant risk. A holistic and individualised risk evaluation approach is crucial for drawing together all terrorism-related data and providing tailor-made suggestions for effectively reducing and/or mitigating the risk of a terrorist attack. Past incidents may provide valuable information concerning the vulnerability of various sites, the potential consequences should an attack materialize, and common tactics used by the aggressors. Clearly, protection of all infrastructures against all threats is impractical in both economic and technical terms, so a cost and benefit analysis needs to be followed for the zones that have to be protected and introduce an efficient protection plan with reduced installation and running costs.

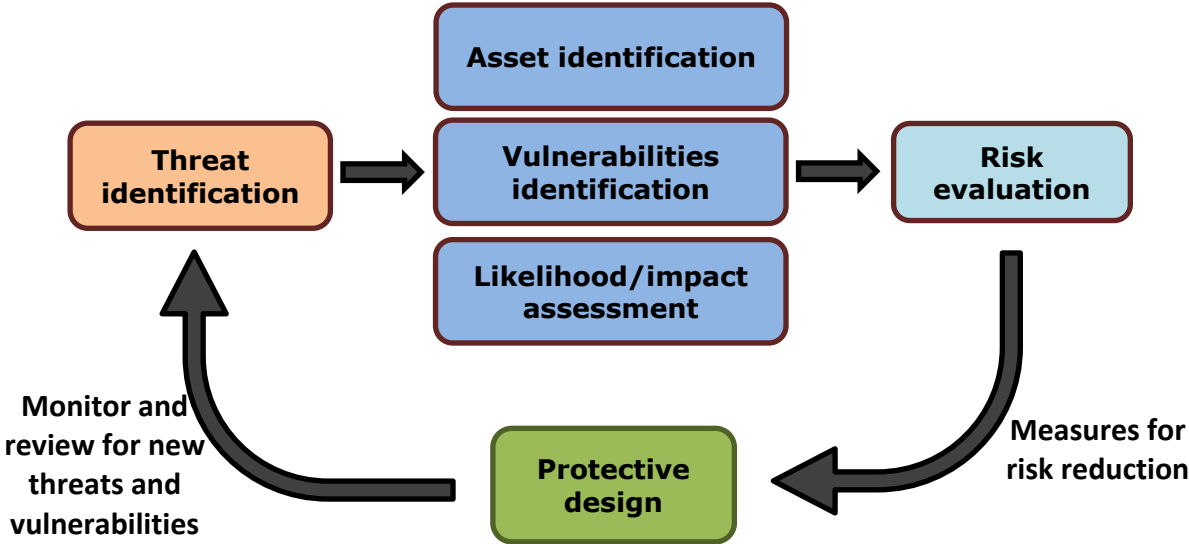
Since a universally accepted risk assessment methodology for terrorism is still missing, efforts should focus on identifying potential threats utilizing available terrorism databases, evaluating the impact of potential attacks and assessing the vulnerability of targets. Terrorism-affected zone maps are available at country level, but breaking down the information to smaller regions is questionable, as the samples usually lack the statistical significance for drawing concrete conclusions. In high terrorist risk countries where many events have occurred in the past there may exist enough data, but in countries with hardly any attacks, as commonly observed in the Western world, this approach leads to unreliable results. However, these zone maps may provide hints regarding the preferred terrorist tactics and potential targets, which are essential inputs for the vulnerability and consequences assessment procedure.

Using the number of fatalities and injuries for assessing the consequences of an attack is a rather straightforward process, as they can be easily measured from prior attacks or even calculated in certain cases (e.g. mortality rate after the explosion of an IED in a crowded place). The use of other parameters, such as the effect of assaults on public morale or the economic damage due to the disruption of services are hard to be measured since they do not constitute quantitative values. Nevertheless, the global targets set out by the Sendai Framework for the disaster risk management include indicators, some of which (e.g. economic loss, disruption of basic services) may be employed during the impact assessment of a terrorist attack.

Finally, the risk assessment process should be updated on a regular basis, since threat types and terrorist tactics alter with time, as shown in Fig. 8. When reviewing terrorism risks different factors, such as the global and local

political scene, religious tensions and the availability of potential weapons (explosives, vehicles, guns, biological agents etc.), should be considered. The various attack scenarios that may be examined during the risk evaluation process should be regularly reassessed and updated to be in line with the latest threat developments. Furthermore, the implementation of mitigation and protective measures need to follow, whenever possible, a security-by-design approach, so that the selected solutions may be harmonically integrated in the surrounding environment, reaching a proper balance between security and the protected asset's characteristics. These measures should focus on increasing the redundancy of the potential target and be effective for a variety of current and emerging threats.

**Figure 8.** Risk and protective design reviewing diagram.



### 3 Protection against attacks with the use of explosives

#### 3.1 General

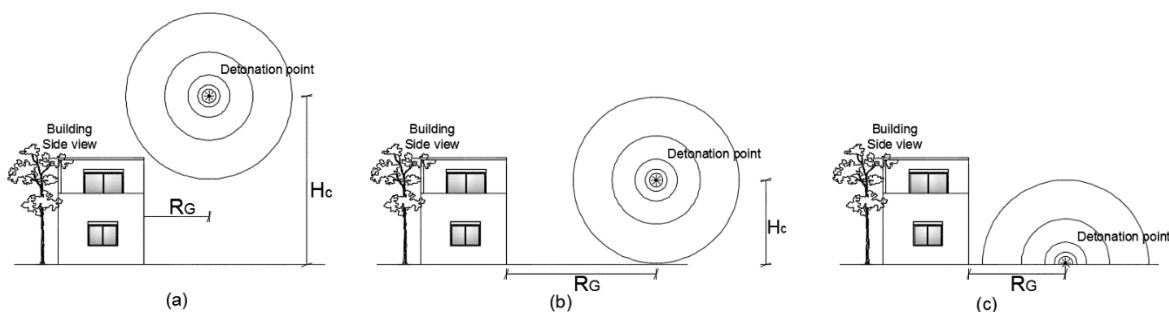
Blast is defined as a very fast chemical reaction involving a solid, dust or gas, during which a sudden release of energy and hot gases takes place. During an explosion the produced hot gases expand and occupy all the available space generating a wave type propagation that grows outwards from the surface of the explosive. Along with the produced gases the surrounding air also expands leading to the creation of a blast wave that impinges on structures located in its path. At the present guideline, the examined blast waves are the result of detonations, since terrorist attacks are usually performed with solid materials characterized by fast reaction rates. This means that the resulting pressures rise nearly instantaneously from atmospheric to their maximum value and rapidly decay in a matter of milliseconds. Only part of the available explosive energy is transformed into blast waves, as the rest of the detonation products mix and burn with the surrounding air. This afterburning process does not affect the produced blast wave as it occurs at a later stage, but should be considered in the case of confined and internal explosions.

Blast waves propagate outwards in all directions (spherically if the explosion takes place in mid-air or hemispherically if the explosive is placed on the ground) at speeds greater than the speed of sound. The front of the blast wave, i.e. the shock front, is characterized by high pressures (or better overpressures as they are calculated in ambient conditions), and their amplitude reduces with increasing distance from the detonation centre, while its duration increases. When the blast wave comes to contact with a rigid surface a reflection occurs that results in increased applied pressures on the surface, known as reflected pressures.

The characteristics of a blast wave at a certain location depend on the distance from the detonation centre, the type and weight of the explosives, and the interaction with the ground or other obstacles situated in its path. Three types of non-contact, unconfined explosions are considered in this guideline, as shown in Fig. 9. Each type depends on the relative position of the detonation centre to the point of interest, i.e. its height from the ground and its horizontal distance between the projection of the explosive to the ground and the structure.

- Free-air bursts:** The charge is detonated in the air and the created blast wave propagates spherically outwards impinging onto the structure without interacting with obstacles or the ground.
- Air bursts:** The charge is detonated in the air and the created blast wave propagates spherically outwards, but before impinging onto the structure it has first interacted with the ground.
- Surface bursts:** The charge is detonated almost at ground level and the blast wave immediately interacts locally with the ground and propagates hemi-spherically outwards before impinging onto the structure.

**Figure 9.** Types of external unconfined explosions: (a) Free-air burst, (b) Air burst, and (c) Surface burst.



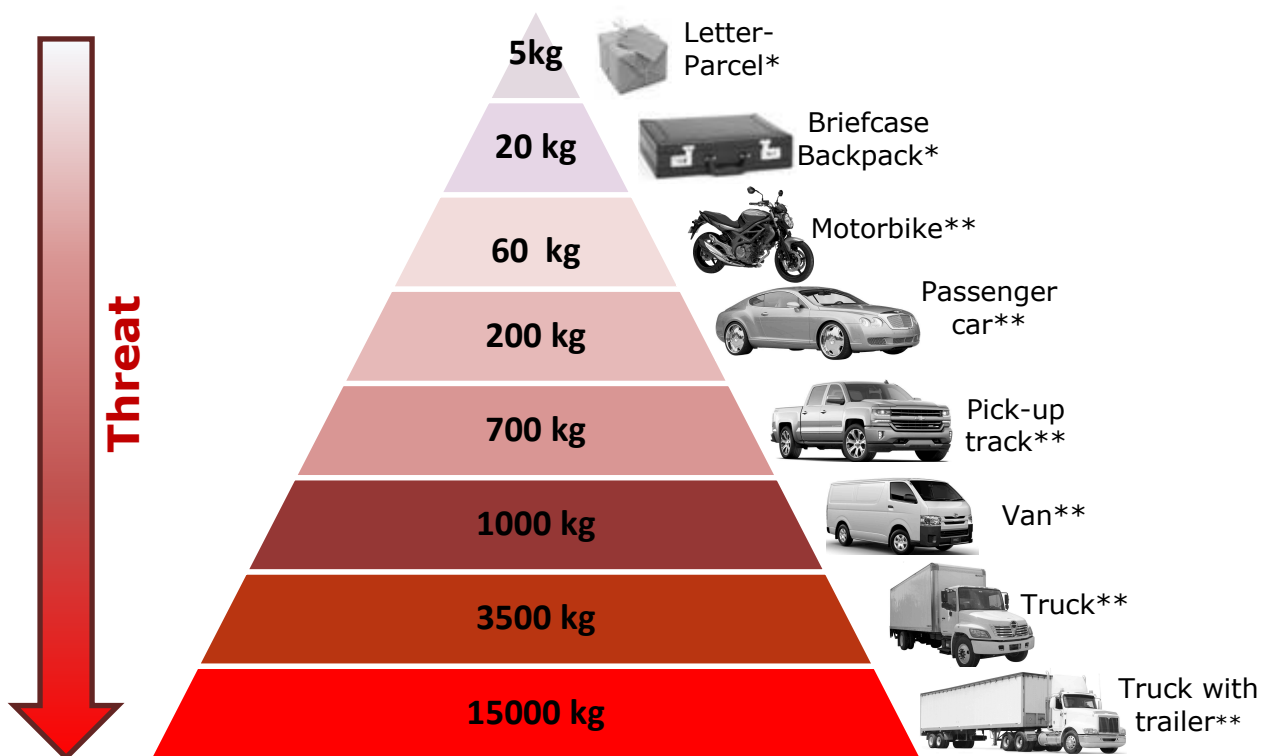
In blast design, localized damage is usually not excluded, as long as it does not jeopardize the safety and load bearing capacity of the structural system and the effects on humans are kept to a minimum. The structure should still be able to fulfil its original purpose with a minimum level of disruption in its use while simultaneously ensuring people's safety. Several strategies exist for reducing the risk of failure and mitigating the effects of an explosion. One option is eliminating or minimizing the probability of occurrence of the action and applying principles of capacity design, such as sacrificial components that are able to reduce the explosion effects

(EN1991-1-7, §3.2.3). Another approach is upgrading the perimeter of a site and increasing the distance of the detonation centre from the target structure decreasing the resulting blast loads. Increasing the strength and ductility of key design members is also an option that results in increased energy absorbing capacity. Also, the presence of alternative load paths in case of member failure, prevents the development of a progressive collapse mechanism (see Section 3.8.3) that could result in a large death toll.

### 3.2 Identifying worst-case scenarios

The probability of a structure or a building to be the target of an explosive terrorist attack is very low, but should not be ignored since the outcome of such an attack could be devastating. The identification of potential targets is a complex and challenging task and requires the analysis of various data, as has already been emphasized in the previous section. Terrorists usually choose their targets desiring to cause human casualties and create a psychological and economic impact to the society. Well-protected targets are often avoided by terrorists, as the chances of a successful attack are lower. An attack scenario may involve weapons, vehicle-borne or person-borne improvised explosive devices. Clearly, the larger the transportation vehicle, the larger the amount of explosives it could transfer and the greater the resulting blast. Fig. 10 shows an estimate of the quantity of explosives that could be carried by various means of transportation.

**Figure 10.** Upper charge mass limit per mean of transportation.



\* Person borne improvised explosive device (PBIED)

\*\*Vehicle borne improvised explosive device (VBIED)

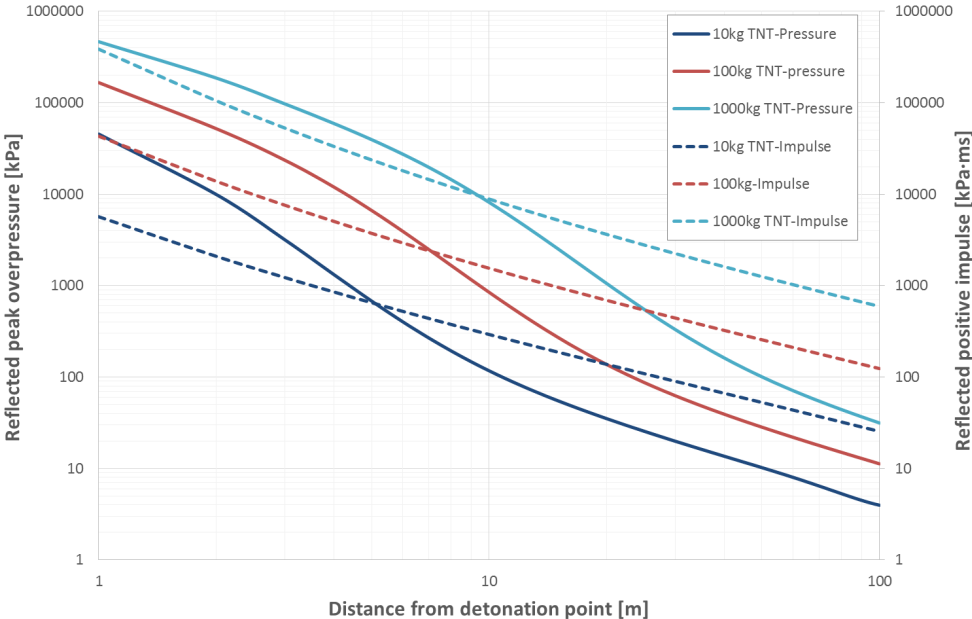
When an attack with the use of explosives is of concern, the charge type and size are usually decided by the building stakeholders and the responsible engineers. The need for a detailed or simplified analysis for an attack scenario depends on a variety of factors, such as the importance of the asset, its occupancy level and the perimeter protection, as has been demonstrated in the previous chapter. This analysis is the base of a well-designed building security plan that can deter intruders from performing an attack and increases the chances of building survival if such an attack materializes.

The consequences of an external explosion to a specific target greatly depend on the stand-off distance, defined as the distance from a possible charge location to the building's façade. As shown in Fig. 11, the explosion energy decreases rapidly with stand-off distance. Hence, increasing the stand-off distance by deploying perimeter protection measures is usually the most economical method for decreasing a site's vulnerability. For example, the use of fences, bollards, walls, planters, trees or other type of barriers prevent the presence of unauthorised vehicles that may carry explosives close to the structure. Clearly, the increase of the distance between the detonation centre and the structure of interest is not always feasible, as in the dense built environment of metropolitan areas, buildings usually occupy nearly all of the available lot, resulting in cases where the perimeter of the field coincides with the structure's façade. The more distant is a building from a city centre, the larger the chances of a bigger lot which translates to bigger space between the building face and adjacent streets and communal spaces.

The stand-off distance value that is utilized in the design process is usually equal to the closest point a vehicle or person can reach from the structure of interest. This is dictated by the abovementioned security measures and could be a point at the fence perimeter (presuming that the fence cannot be breached), a parking spot near the building, a location in a square or atrium in front of the building etc. Consequently, the first step towards defining the potential detonation centre to be inserted in the blast design study, is the evaluation of the surrounding area characteristics. The site topography, meaning the location of the building in comparison to its surroundings, is important for evaluating the opportunities the aggressors might have to strike.

Fig. 11 shows the normal peak reflected pressure and normal reflected impulse at a point with respect to the distance from the detonation centre for a hemispherical blast wave from the explosion of 10kg, 100kg and 1000kg of TNT. The diagrams are produced following the equations proposed by (Kingery, Bulmash, 1984). The plots show that a small increase in the stand-off distance results in large reduction in pressure and impulse values for all charge weights. Furthermore, the decrease rate of peak pressure values is larger than that of the positive impulse for the whole distance range.

**Figure 11.** Peak reflected pressure and reflected impulse versus stand-off distance.



The protection measures that are deployed at the perimeter of a building are also important when defining the charge weight for the design process. For explosive devices of substantial size that have to be transported by a vehicle (Vehicle Improvised Explosive Devices-VBIEDs) the stand-off distance is usually calculated from the closest point to the structure accessible by a vehicle, such as the fence, the access control point etc. The closest point to a structure may not coincide with the worst-case scenario for a specific component, since the blast wave energy at a location is also dependent on the angle of incidence, as will be shown later. Therefore, the critical detonation point should be defined taking into consideration both its stand-off distance and its relative location to the structure. Clearly, the security measures are expected to fulfil their purpose so that the hostile vehicle cannot breach the site premises, by either penetration, deception or other techniques. Similarly, the



critical point for the case of a person-borne improvised explosive device (PBIED) should be determined according to the site public accessibility. In that case, the charge mass is substantially lower than that of a VBIED.

### 3.3 Explosive materials

As already mentioned, the design of a structure against blast induced loads is accompanied by a risk assessment study that is dependent on the unique characteristics of each project. Part of the risk assessment is the identification of the type and weight of the explosives that are utilized for the calculation of the blast parameters. Due to the several types of explosives that are available today, any of which could be used for constructing an explosive device, the universal quantity of TNT (Trinitrotoluene) has been adopted for all necessary computations. An equivalent TNT weight is calculated that produces the same explosive energy, peak pressure or positive impulse to that of the weight of the actual unconfined explosive. This way the effects from various explosives and different blast experiments can be compared, as they are conveniently linked to an equivalent TNT weight.

One way of assessing the equivalent TNT weight is by utilizing the heat produced during the detonation, a quantity indicating the energy content of the explosive material. Proposed values can be found in the open literature (UFC 3-340-02, 2008) (U.S. Department of the Army, 1990) and substituted in the following equation,

$$W_e = E_{exp} \frac{H_{exp}^d}{H_{TNT}^d} \quad (1)$$

where:

$W_e$  is the TNT equivalent weight [kg],

$W_{exp}$  is the weight of the actual explosive [kg],

$H_{exp}^d$  is the heat of detonation of the actual explosive [MJ/kg], and

$H_{TNT}^d$  is the heat of detonation of the TNT [MJ/kg].

Table 4 contains predetermined TNT equivalent weight factors to be applied directly at the charge weight of the actual explosive (IATG, 2011 and Dusenberry, 2010 and Pachman et al. 2014 and TM5-855-1, 1997 and ASCE 2011). This way a TNT weight is determined that produces the same blast parameters as the ones of another explosive of a certain weight. As shown, the TNT equivalence factor may be different depending on the parameter that is used for the transformation (peak pressure or positive impulse). This means that the equivalent factor should be chosen based on the parameter that is critical for the examined structure. If, for instance, the duration of the excitation  $t_o$  is expected to be much shorter than the natural period of the structure ( $\omega_n t_o < 0.4$ ), then one deals with impulsive loading and the equivalence factor should be selected accordingly, where  $\omega_n$  is the structure's natural frequency. The factors included in Table 4 are valid over certain shock front pressure ranges which are rather low, which means that the proposed transformation factors may prove inaccurate for close-in detonations where the blast phenomenon is more complex due to the expanding detonation products.

**Table 4.** Equivalence TNT factors (various sources).

<b>Explosive</b>	<b>Density (g/cm<sup>3</sup>)</b>	<b>TNT equivalent weight factor (Pressure)</b>	<b>TNT equivalent weight factor (Impulse)</b>	<b>Pressure range (MPa)</b>
<b>TNT</b>	<b>1.61</b>	<b>1.00</b>	<b>1.00</b>	<b>standard</b>
AMATOL	NA	0.99	0.98	NA
Ammonia dynamite (50% strength)	NA	0.90	0.90	NA
Ammonia dynamite (20% strength)	NA	0.70	0.70	NA
ANFO (nitrate/fuel 94/6)	NA	0.82-0.87	0.87	0.03-6.90
Composition-A-3	1.65	1.09	1.07	0.03-0.35
Composition-B	1.65	1.11 1.20	0.98 1.30	0.03-0.35 0.69-6.90
Composition-C3	1.60	1.05-1.08	1.01-1.09	0.035-0.350
Composition-C4	1.59-1.71	1.37	1.19	1.38-20.70
CYCLOTOL (RDX/TNT 60/40) (RDX/TNT 70/30)	1.68 1.14	1.04 1.14	1.16 1.09	0.035-0.35
DATB	1.79	0.87	0.96	NA
Explosive D	1.71	0.85	0.81	0.007-0.30
HBX-1	1.76	1.17	1.16	0.03-0.14
HBX-3	1.85	1.14	0.97	0.03-0.17
HMX	1.91	1.02	1.03	NA
MINOL II	1.83	1.20	1.11	0.02-0.14
NITROCELLULOSE	1.65-1.70	0.50	0.50	NA
NITROGLYCERINE DYNAMITE (50% strength)	1.60	0.90	0.90	NA
NITROMETHANE	1.13	1.00	1.00	NA
OCTOL (HMX/TNT 75/25)	1.81	1.02-1.06	1.06	NA
PBX-9010	1.80	1.29	1.29	0.03-0.21
PBX-9404	1.81	1.13 1.70	1.13 1.70	0.03-0.69 0.69-6.9
PBXN-4	1.71	0.83	0.85	NA
PBXN-107	1.63	1.05	1.05	NA
PBXW-125	1.79	1.02	1.02	NA
PETN	1.77	1.27	1.11-1.27	0.03-0.69
RDX	1.76-1.81	1.10-1.14	1.09-1.10	NA
RDX/WAX (98/2)	1.92	1.16	1.16	NA
RDX/AL/WAX (74/21/5)	NA	1.30	1.30	NA
TATB	NA	1.00	1.00	NA
TATP	1.20	0.70-0.80	0.55	NA
TETRYL	1.71-1.73	1.07	1.05-1.07	0.021-0.140
TETRYTOL (TETRYL/TNT 75/25)	1.59	1.06	1.06	NA
TNETB	1.69	1.13-1.36	0.96-1.10	0.03-0.69
TROPEX	1.84	1.23	1.28	0.007-0.30
TRITONAL (TNT/AL 80/20)	1.72	1.07	0.96	0.03-0.69

### 3.4 Loading definition

Blast loading is mentioned in the Eurocodes, the European standards specifying rules and regulations for the structural design of various engineering structures. In detail, Eurocode EN1991-1-7 (EN1991-1-7, 2006) makes reference to the case of accidental actions that result in exceptional dynamic loads that should be considered in design if there shall be a reasonable probability of significant damage to the structure. These design situations can result from natural causes, malpractice, accidents or terrorist attacks. The latter are difficult to be predicted, since they depend on the individual competencies of the attackers. Unless otherwise specified, blast actions should be considered dynamic, accidental design situations which refer to exceptional conditions applicable to the structure or to its exposure as laid out in EN 1990, §3.2 and EN 1990, §4.1.1. The blast actions should be considered to act simultaneously with other permanent and variable actions, as described in EN1990, §6.4.3.3 using the relevant combination coefficients.

There exist a number of loads that can be considered of high dynamic nature, such as impact, blast, penetration. The analysis and the simulation options of such loads are more complex than the ones for static loading. High dynamic loads cause significantly higher strain rates than other dynamic loads (e.g. earthquakes) and are usually rare, but their influence on structures or components should not be neglected, since they could lead to large casualties and structural failure. Such high dynamic loads are:

- **Impact:** Impact is usually defined as a large force that acts over a very short period of time after the collision of two or more objects. The results of an impact depend on both the characteristics of the impactor and the properties of the target structure. The higher the velocity, the size and the stiffness of the impactor, the more damage it could cause. Clearly, the damage to the target depends on its material, its type, its size etc. A car, train or airport crash, a ship collision against a bridge pier, the fall of a mobile phone on the ground are examples of common impact loading events. Simulating such problems is quite complex as the phenomenon usually combines high velocities, large deformations, friction effects etc. If one body with an initial velocity collides with another being at rest, two extremes can be distinguished as proposed by Eibl (Eibl, 1987) and CEB (CEB, 1988): soft and hard impact. At the former case the kinetic energy of the impacting body is totally transformed into deformation of the same body, while the resisting mass remains practically undeformed. During hard impact, the kinetic energy of a rigid impactor is absorbed (partially or totally) by the deformation of the second body. This means that the dissipation of energy at soft impacts takes place mainly at the impactor, whereas at hard impacts it is the colliding body that deforms and absorbs the energy.
- **Explosion:** Explosions last only some milliseconds and are the result of accidental or intentional detonation or deflagration of explosive materials. Detonations are characterized by the creation of a wave propagating at supersonic speeds resulting in high overpressures while the wave created during deflagrations propagates at subsonic velocities and has smaller overpressures. The current guideline focuses for simplicity on explosions that take place in the open air after the detonation of a spherical charge. The pressure-time history of internal explosions is more complex as due to the confinement effect, pressures are repeatedly reflected from the various surfaces. In addition, due to the afterburning effect the overpressures might be amplified after their initial peak value. Some guidance on the analysis of internal explosions is provided in the Eurocode EN 1991-1-7 (EN1991-1-7, 2006). For charge shapes besides spherical, some differences are expected from the values that are proposed subsequently, and in particular in the near field. The military, mining and construction communities use charges whose shape varies significantly from that of a sphere, as for example in the cases of shaped charges that are designed to focus their energy for a specific objective (i.e. penetration).
- **Contact detonations:** At close-in or contact detonations, the explosive material is very near or in contact to a structural component respectively, as in the case of hand-carried explosives that are usually placed adjacent to a component. The failure mechanisms differ from other type of explosions (Remennikov A. et al., 2015), as the generated high-intensity blast loads are applied over a small area and the resulting failures are usually localized and might not affect the whole structure. Contact explosions have similar characteristics to penetration and perforation phenomena, such as those following a projectile colliding with a wall and may provoke breach, brisance or shear failures. In case of such type of events, the structure should exhibit adequate redundancy for redistributing the gravity loads through alternative load paths.
- **Fragmentation and penetration:** The detonation of a charge may be accompanied by the creation and dispersion of fragments that are either part of the casing or have been included intentionally in

the explosive to increase the number of fatalities. Usually these fragments are made of metal and can travel at high velocities causing injuries and damaging structures that are situated at a relatively short distance from the detonation point. For rigid structures (reinforced concrete, steel etc.) the resulting penetrative damage is usually localized at the surface and combined with the blast wave may result in more extensive failures depending on the timing of the arrival. Lighter structures might be penetrated from the produced fragments and cracking may appear. Typical examples of explosives characterized by these two aspects are military weapons and bombs.

### 3.5 Blast wave parameters

The majority of the blast wave parameters that characterize a blast wave are described in Fig. 12, which shows the ideal pressure-time curve at a point located at a certain distance from the detonation centre. The amplified reflected overpressures are attributed to the nature of the propagation of the blast wave through the air. The particles that are carried by the blast wave along its path collide with the surface upon arrival but cannot bounce right back due to the subsequent particles that follow, leading to greater values of reflecting pressures. The main parameters in Fig. 12 are:

- a. The peak positive incident (or side-on) overpressure  $P_{so}$  and the peak reflected pressure  $P_r$ ,
- b. The positive phase duration  $t_o$ ,
- c. The positive incident  $i_{so}$  and reflected  $i_r$  impulse, calculated by integrating the positive phase incident and reflected pressure-time curves respectively,
- d. The arrival time  $t_A$ , measured from the time of detonation,
- e. The peak negative incident (or side-on) overpressure  $P_{so}^-$  and the peak negative reflected pressure  $P_r^-$ ,
- f. The negative phase duration  $t_o^-$ ,
- g. The negative incident  $i_{so}^-$  and reflected  $i_r^-$  impulse, calculated by integrating the negative phase incident and reflected pressure-time curves respectively,
- h. The stand-off distance  $R$  between the point of interest and the detonation centre (not included in Fig. 12),
- i. Additional parameters (not included in Fig. 12) are the positive  $L_w$  and negative  $L_w^-$  blast wave length and the shock wave speed  $U$ . The positive blast wavelength is equal to the distance that takes the shock wave pressure to decay from its maximum to ambient value and depends on the shock wave speed and the positive duration.

As stated before, Fig. 12 shows the pressure-time history of an ideal blast wave, which means that the distance of the point of interest to the blast source is not very small. For close-in or contact explosions, the shape of the pressure-time history is different from the idealized form presented in Fig. 12 due to the effect of the expanding detonation products.

The pressure after its peak value decays exponentially until it reaches the ambient pressure. This phase, widely known as positive phase, is linked to the majority of structural and non-structural damage. After this positive phase, the pressure becomes smaller than the ambient value, before finally returning to it. This part of the diagram is referred to as negative phase and is usually not taken into account for design purposes as it is characterized by much smaller pressure and impulse values. The decay of the idealized pressure-time curve of Fig. 12 is usually represented through the modified Friedlander equation,

$$P_s(t) = P_{so} \left(1 - \frac{t}{t_o}\right) e^{-b\frac{t}{t_o}} \quad (2)$$

where:

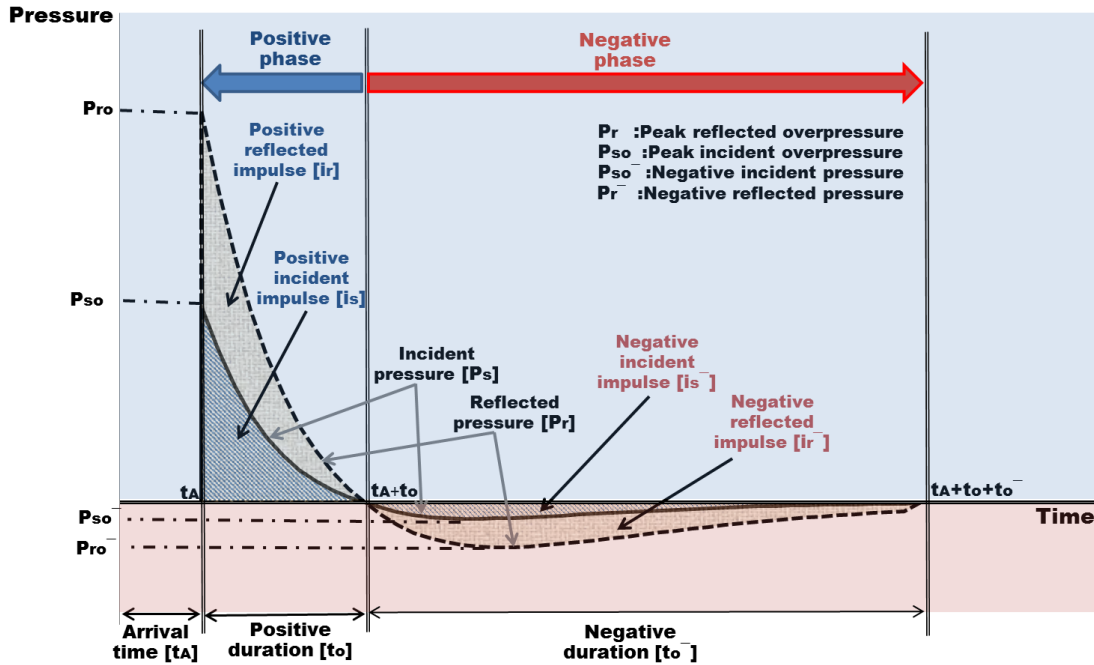
$b$  is the decay coefficient of the waveform, and

$t$  is the time elapsed, measured from the instance of blast arrival.

Clearly, the reflected parameters are the ones to be used for the design of surfaces (e.g. walls, windows) that are not parallel to the propagation direction of the blast wave. The reflected pressure can be several times greater than the incident pressure depending on the structure's geometry, type, size, weight and distance of the

explosive device, the relative location of the detonation centre to the surface under examination, the interference of other obstacles in the wave's propagation direction etc.

**Figure 12.** Incident and reflected pressure time histories.



### 3.6 Scaling laws

The blast parameter values and equations that are proposed by various researchers are based on large experimental databases. For generalizing the experimental results to include cases that are different from the initial setup, scaling laws have been introduced, that allow the blast parameters to be used for varying values of distance and charge energy release. The most commonly used approach is known as the “cube root” scaling law and was established independently by (Hopkinson, 1915) and (Cranz, 1926), introducing a dimensional scaled distance as described by,

$$Z = \frac{R}{\sqrt[3]{W}} \quad (3)$$

where:

$R$  is the stand-off distance [m], and

$W$  is the weight of the actual explosive [kg].

### 3.7 Calculation of blast loads

#### 3.7.1 Free-air bursts

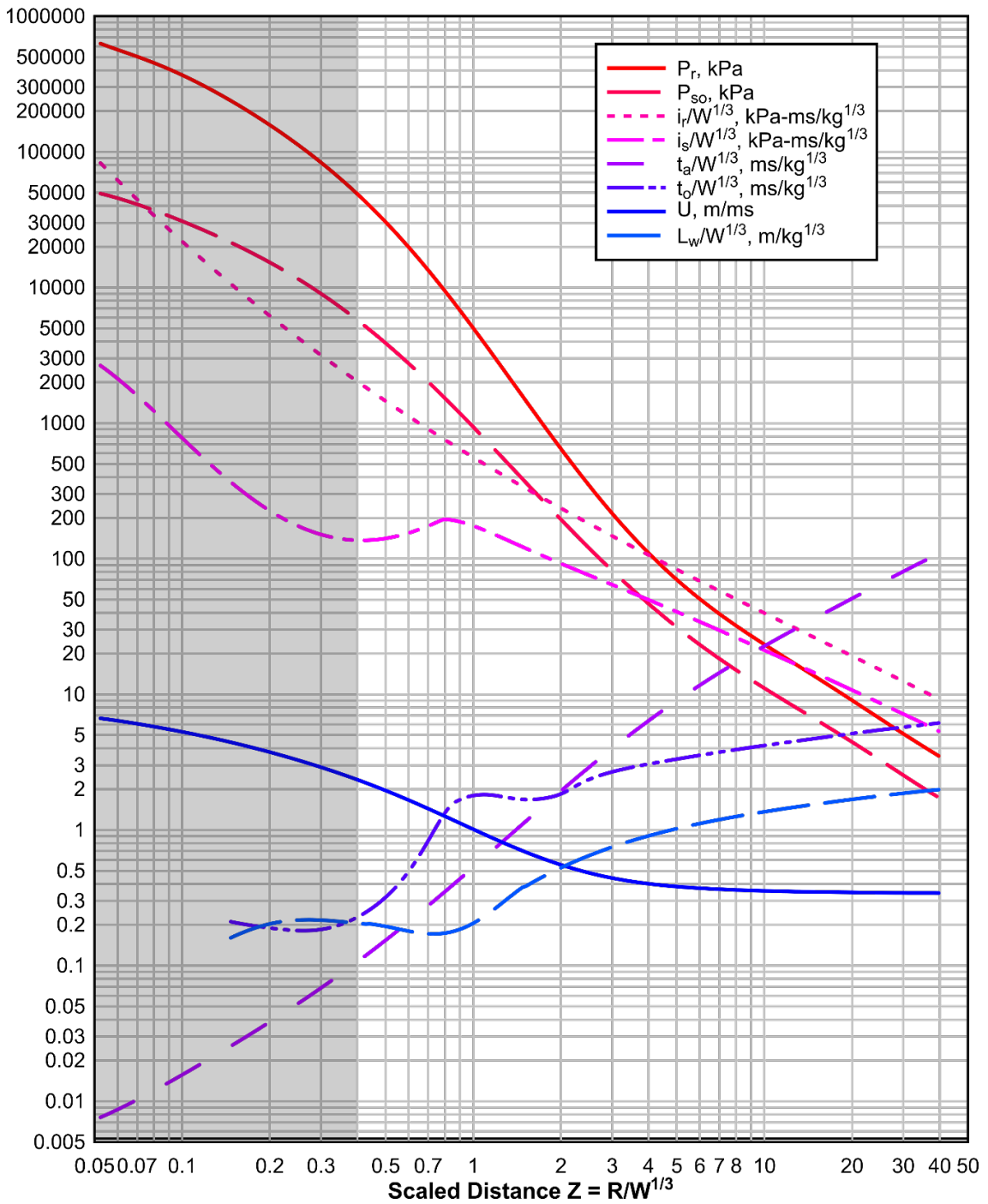
During a free-air burst, the explosion takes place in the air and a spherical blast wave is produced. Since no obstacles stand between the detonation centre and the point of interest, the blast wave will impinge on the examined surface without any amplification. Upon impact to the surface, the initial blast wave will be reflected

and its pressure and impulse will be reinforced. If the surface is perpendicular to the propagation direction of the blast wave, normal reflection takes place, which is usually characterized of maximum pressure and impulse values. In the following diagrams, the reflected parameters refer to normal reflection conditions.

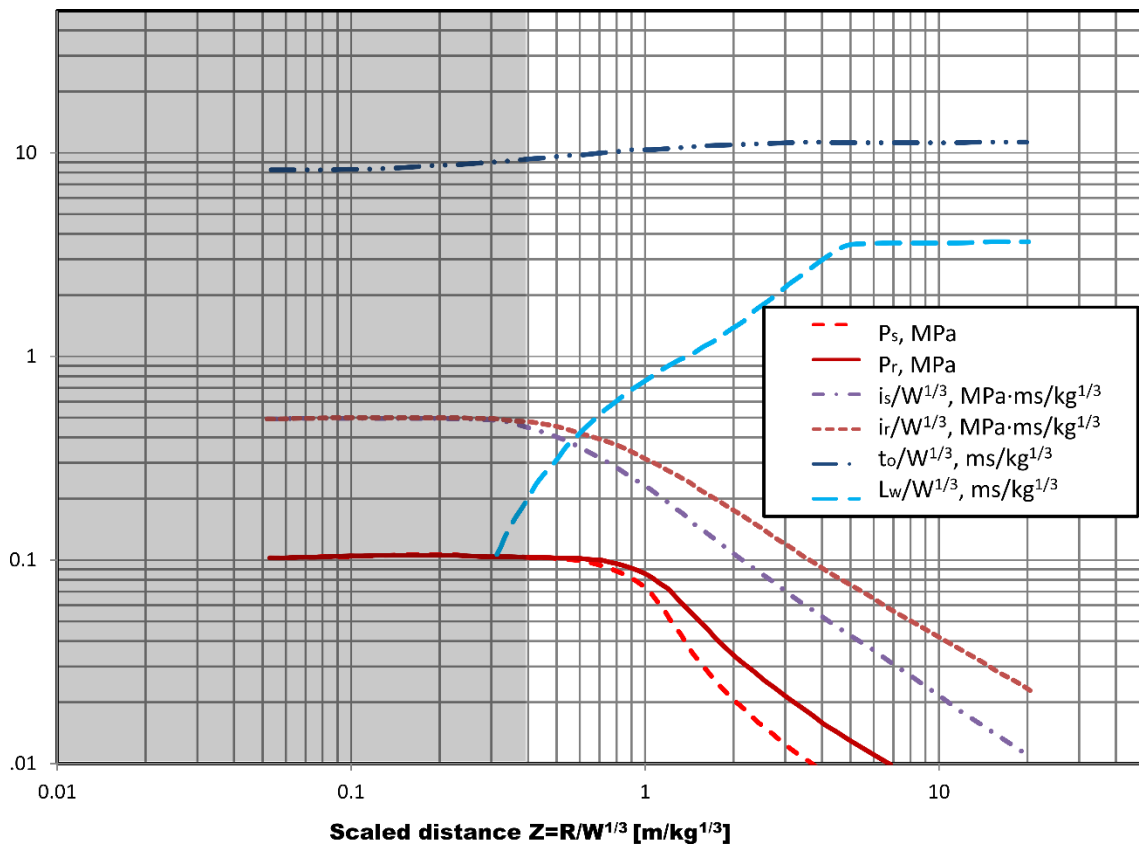
There are many relationships for determining the incident pressure and impulse values at a specific distance from an explosion. These equations have been studied in the past by various researchers (Karlos et al. 2016, Aleem et al. 2016, Goel et al. 2012, Shin et al. 2015) who concluded that big differences might appear, especially at small scaled distances. In the present guideline, the determination of the blast parameters as proposed by Kingery and Bulmash (Kingery, Bulmash, 1984) is employed. Their formulations are dependent on the logarithm of the scaled distance. They are the most widely used and accepted equations, as they have been included in many blast design technical manuals, including (TM 5-1300, 1990 and UFC 3-340-02, 2008). Fig. 12 and Fig. 13 show the diagrams of the blast parameters for the positive and negative phase of a spherical blast wave respectively. The diagrams are the metric-units rendition of the curves contained in (TM 5-1300, 1990) and (UFC 3-340-02, 2008) and have been drawn in respect to the scaled distances from  $Z=0.05\text{m/kg}^{1/3}$  to  $Z=40\text{m/kg}^{1/3}$ . From these diagrams in order to obtain the absolute value of each parameter, its scaled value has to be multiplied by a factor  $W^{1/3}$  to take into account the actual size of the charge, apart from pressure and velocity quantities that are not scaled. It is reminded that the parameters of the negative phase of the blast wave (Fig. 13) are usually not taken into account for the design of rigid structures, but should be considered for more flexible ones at relatively large scaled distances (Krauthammer and Altenberg 2000, Rigby et al. 2014, Teich and Gebbeken 2010).

The blast parameters proposed by Kingery and Bulmash at small scaled distances, should be treated with caution as there exist big uncertainties (Shin et al. 2015, Bogosian et al. 2002, Smith et al. 1994). For contact or close-in detonations where violent outflows and afterburning phenomena may take place, the supporting experimental data are limited and of ambiguous quality and the pressure-time curves do not follow the simple pattern with the single peak and the exponential decay (Friedlander equation). Blast parameter values at scaled distances smaller than  $0.4\text{m/kg}^{1/3}$  should be adopted with conservatism (greyed area of Fig. 13 and Fig. 14).

**Figure 13.** Parameters of positive phase of shock spherical wave of TNT charges from free-air bursts (modified from UFC 3-340-02, 2008).



**Figure 14.** Parameters of negative phase of shock spherical wave of TNT charges from free-air bursts (modified from UFC 3-340-02, 2008).



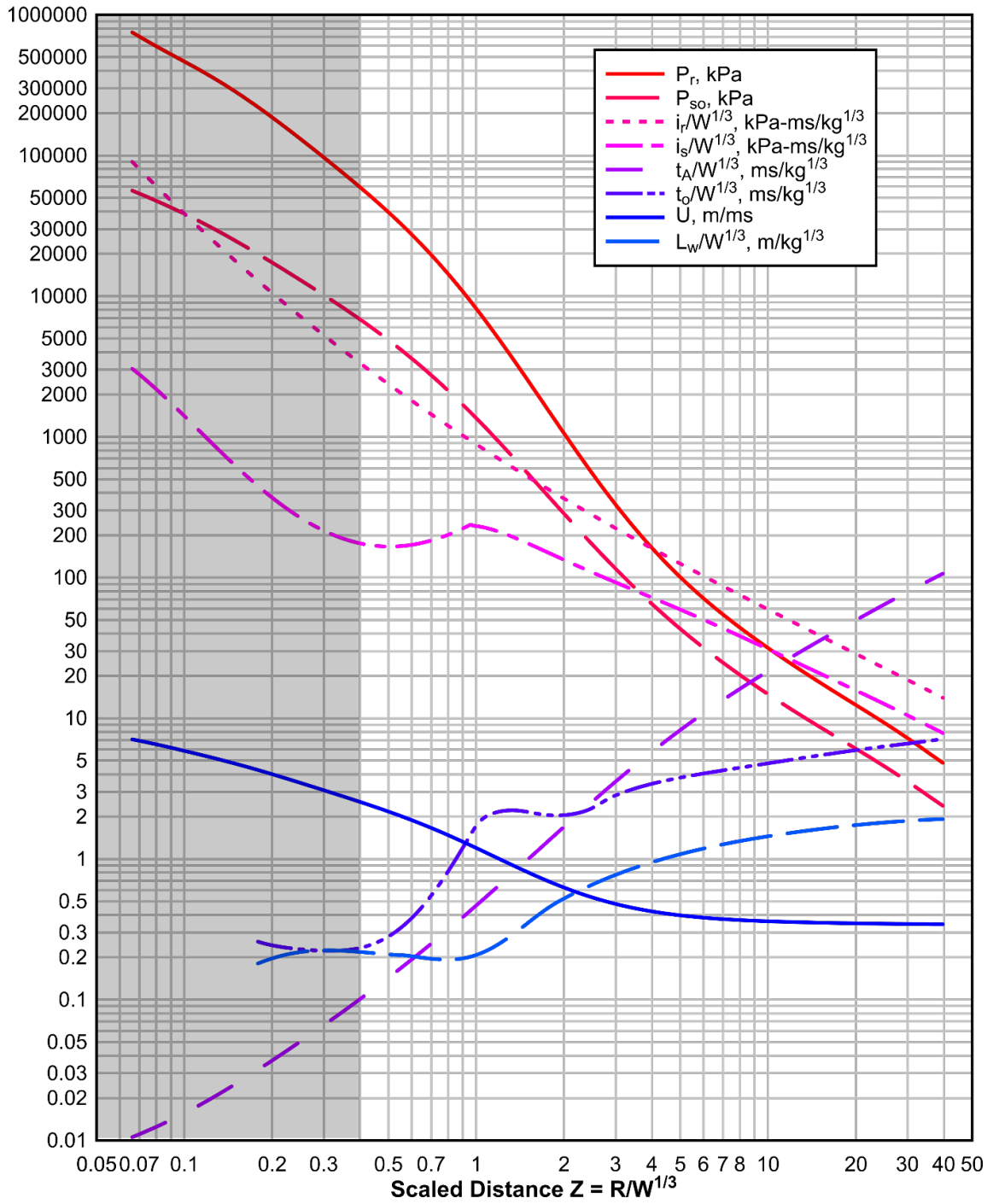
### 3.7.2 Surface bursts

As the charge is placed at ground level (or very near the ground), the produced blast wave reflects instantly off the ground surface forming a hemispherical blast wave resulting in higher pressure and impulse values than those presented in Fig. 13 and Fig. 14. Surface explosions are very common in both intentional and unintentional explosions since the explosives are usually positioned on the ground (vehicles, containers, storage facilities etc.).

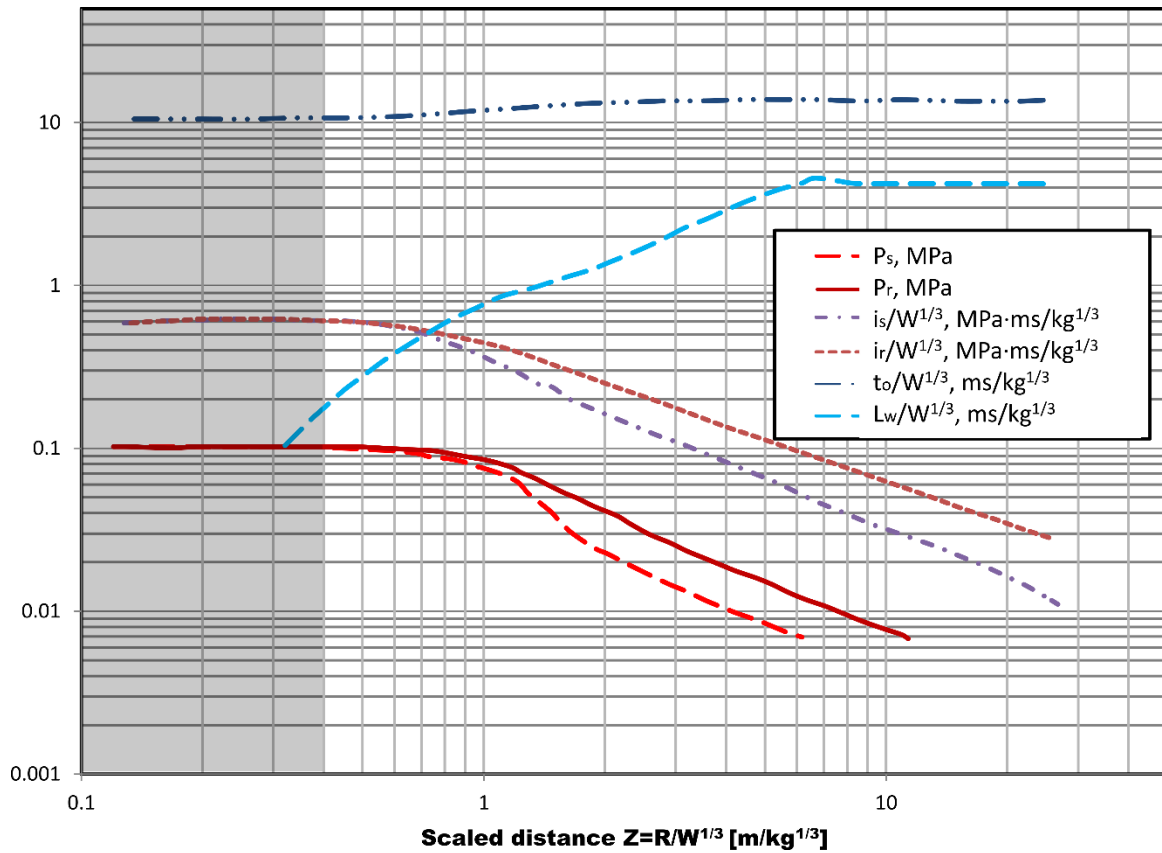
Fig. 15 and Fig. 16 show the positive and negative phase blast parameters for a hemispherical TNT explosion respectively. It is noted that part of the energy produced during the detonation is absorbed from the ground, resulting in the creation of a crater.



**Figure 15.** Parameters of positive phase of shock hemispherical wave of TNT charges from surface bursts (modified from UFC 3-340-02, 2008).



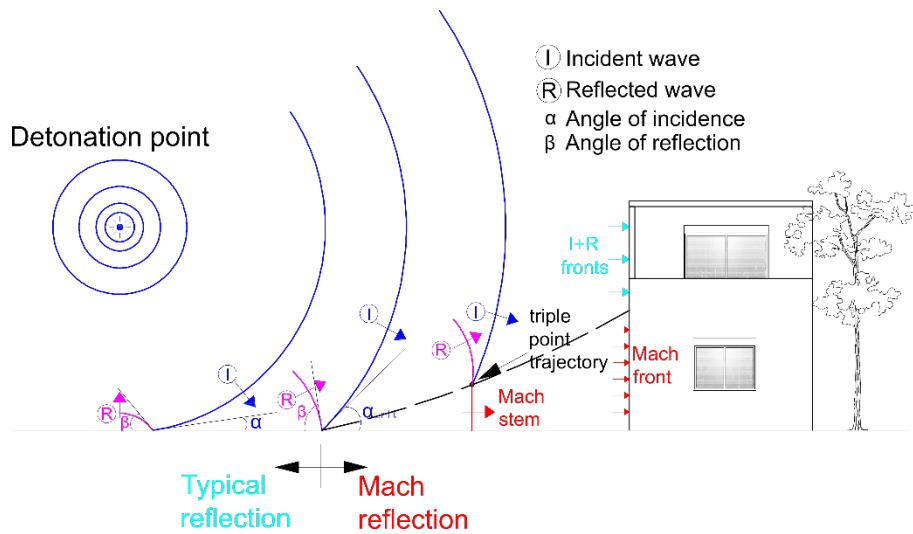
**Figure 16.** Parameters of negative phase of shock hemispherical wave of TNT charges from surface bursts (modified from UFC 3-340-02, 2008).



### 3.7.3 Air bursts

Air bursts combine aspects from both surface and free-air bursts, as the explosion takes place near the ground and the initial spherical blast wave interacts with the ground before coming to contact with the examined surface, as shown in Fig. 17. The blast wave is made up of an incident wave, emanating from the explosive charge, and of a reflected wave, which is produced from the reversal due to the impingement of the wave to the ground. As the blast wave propagates, the incident and the reflected wave merge and front, commonly referred to as Mach front, is created as shown in Fig 17. This new wave is the product of the reinforcement of the incident wave after impinging on the ground. The point of intersection of the incident, reflected and Mach front is known as triple point.

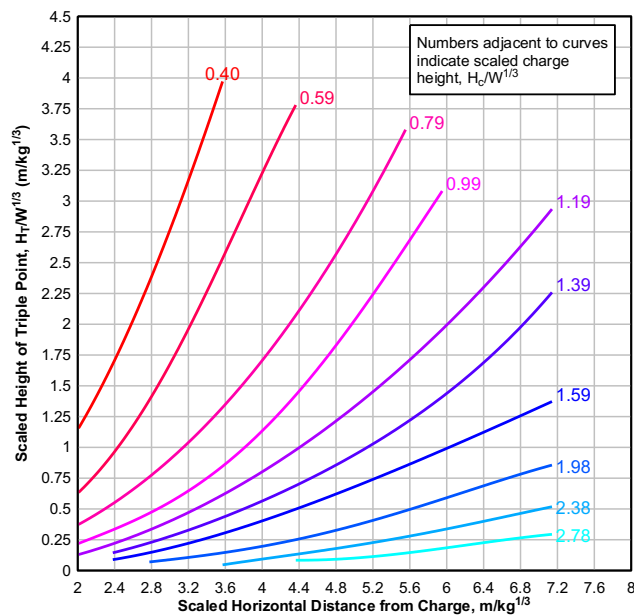
**Figure 17.** Formation of Mach front and triple point due to a near ground explosion.



If the height of the triple point, shown in Fig.17, exceeds the height of the structure, the whole surface is loaded by the Mach front, which is considered plane. If the height of the triple point is less than the height of the structure, then the part of the surface below the triple point is loaded by the Mach front and the part above the triple point is loaded by a combined incident and ground reflected blast wave. The pressure and impulse values above the triple point are smaller than those of the Mach front, so it is on the conservative side to assume that the whole surface is loaded by the Mach front.

The pressure and impulse values at the bottom of a structure (Mach front) are dependent on the angle of incidence of the blast wave. Practically in most cases the detonation centre is at such a distance, that the structure is loaded only by the Mach front. The procedure for calculating the complex loading time history of a structure under an air burst can be located in [Baker et al. 1983, TM 5-1300, 1990 and UFC-3-340-02, 2008].

**Figure 18.** Estimation of Mach front height  $H_T$  from the scaled charge height  $H_c/W^{1/3}$  and scaled horizontal distance  $H_c/W^{1/3}$ .



### 3.7.4 Effect of angle of incidence

The diagrams utilized for the calculation of the reflected blast parameters are valid if the blast wave travels perpendicular into the affected surface. If there is an angle  $\alpha$  (angle of incidence) between the propagation direction and the surface of interest, as shown in Fig. 19, the reflection process is different and affects the magnitude of the reflected pressure and impulse.

**Figure 19.** Angle of incidence at a building face.

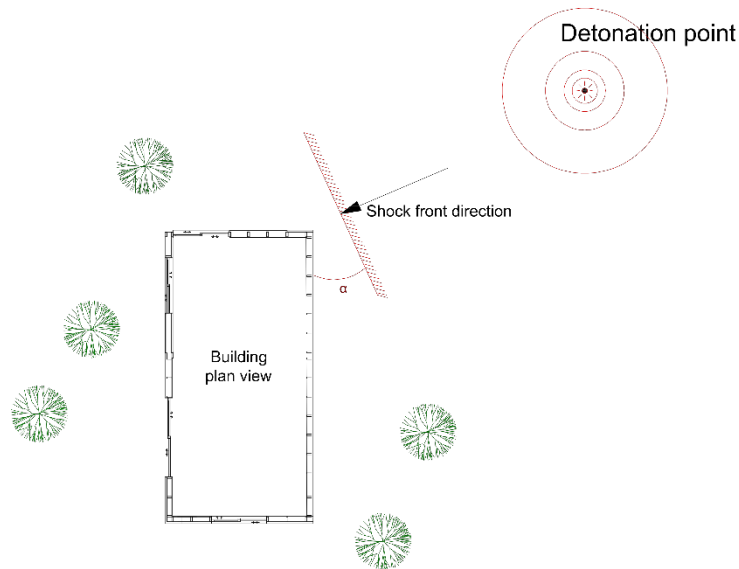
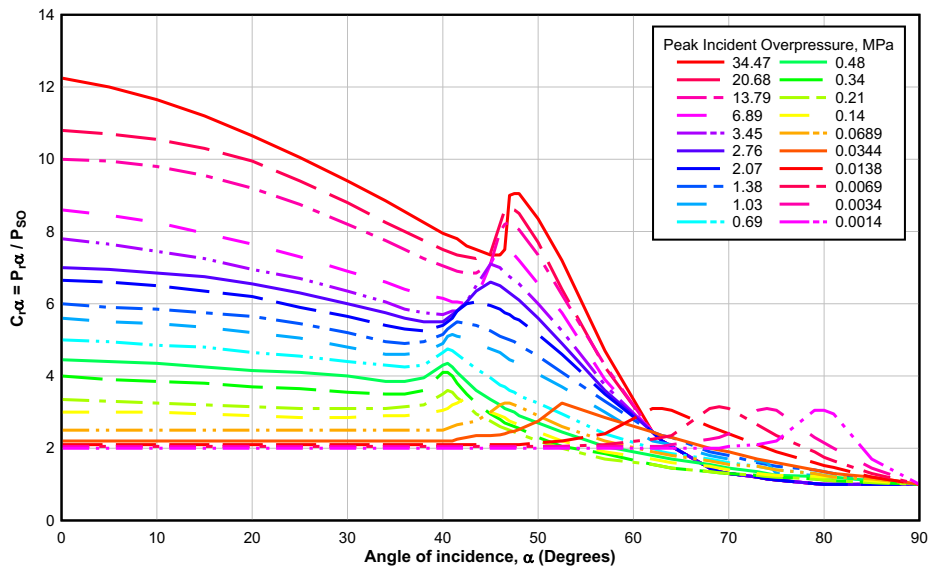


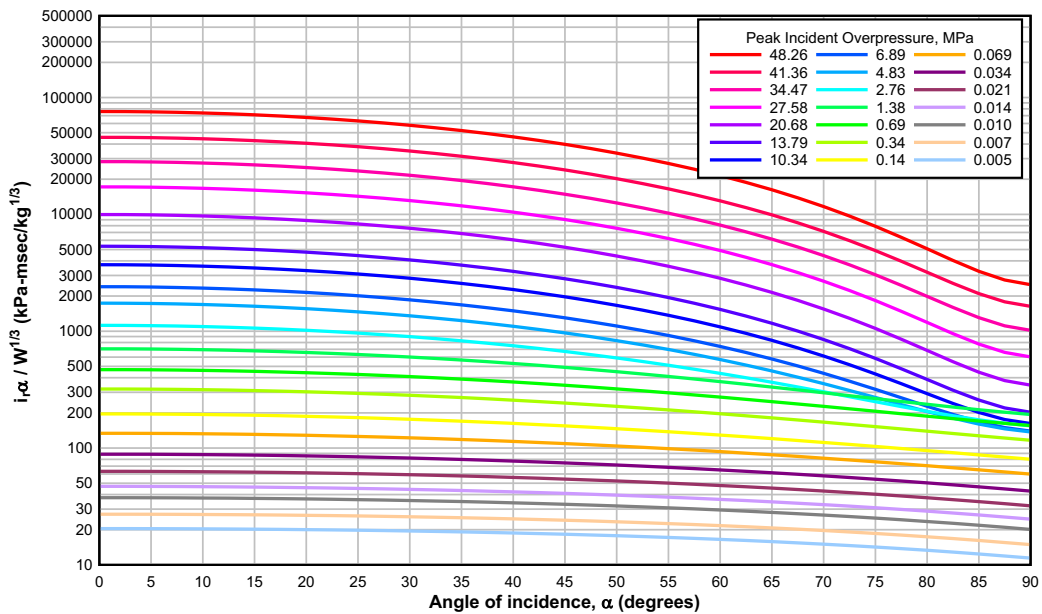
Fig. 20 shows the influence of the angle of incidence on the ratio of the peak reflected overpressure to the peak incident overpressure. If the obstructing surface is parallel to the direction of the blast wave, the reflected pressure is equal to the incident one as no amplification takes place and if the surface is perpendicular to the propagation direction, normal reflection occurs. As shown in Fig. 13 and Fig. 15 the larger the explosion, the higher the amplification of the incident pressure after the reflection process. It is usually on the conservative side to neglect the effect of the angle of incidence and study a structure under normal reflection conditions, especially in the case of large incident overpressures. The pattern of the curves for angle of incidence values above  $40^\circ$ , is attributed to the creation of a Mach stem, which forms when the incident and the reflected wave coalesce. The Mach front pressure-time history is similar to the one of the incident pressure and is described by the Friedlander equation.

**Figure 20.** Influence of the angle of incidence on the ratio of reflected to incident overpressure (modified from UFC 3-340-02, 2008).



Similar to Fig. 20, the positive reflected impulse  $i_{r,\alpha}$  values are also affected by the angle of incidence and can be conveniently calculated from Fig. 21. The relevant curves are valid for free-air bursts and spherical blast waves.

**Figure 21.** Influence of the angle of incidence on the positive reflected impulse (modified from UFC 3-340-02, 2008).



### 3.7.5 Clearing effects

The proposed reflected pressure and impulse values are valid in the case of a blast wave acting on an infinite surface. However, near the edges of a building or in the presence of openings to the reflecting surface, these values may reduce as the expanding air can flow around the sides of the surface. This means that the resulting pressures are relieved depending on the blast wave speed, the distance of the measuring point from the free edge (surface geometry) and the pressure magnitude. The peak overpressure is identical for both infinite and finite surface conditions, but the decay rates are not identical resulting in different positive duration and impulse

values. Clearly, it is on the conservative side to consider infinite conditions when studying the effect of a blast wave on a surface, especially if its response depends mainly on the produced impulse.

Modern buildings are characterized by an extended use of large openings to ensure lightening and ventilation of the internal spaces. The use of façades made entirely out of glass is a popular element in contemporary architectural design. Glass panels are the first to fail following an explosion, as they usually constitute the most vulnerable part of the structural face. Even if they are designed to sustain the blast wave, the current philosophy behind structural design dictates that they form the weakest part of the wall system, since an eventual failure of the wall before failure of the glass panels is considered more dangerous.

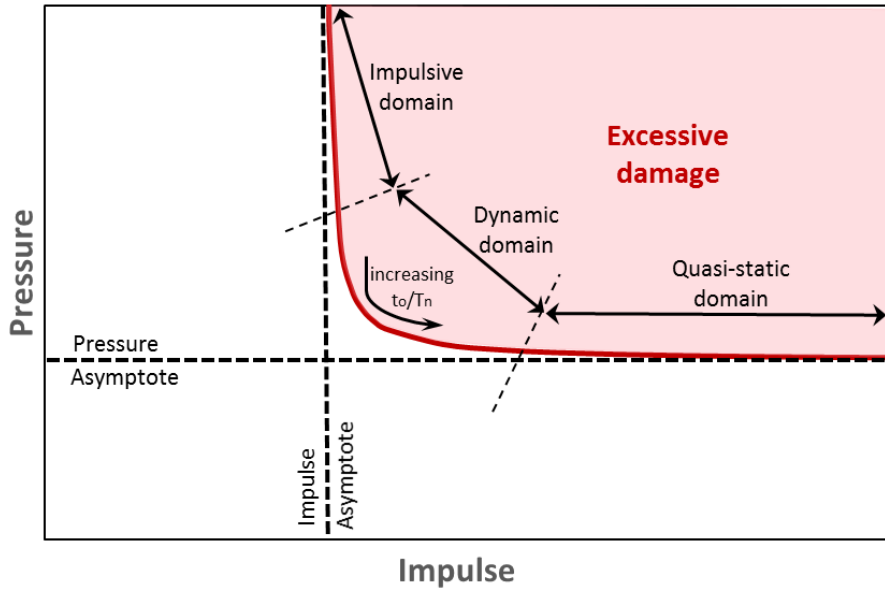
When the shock front comes to contact with a window, it will instantly cause its failure and will propagate at the building's interior. The peak pressure value will become smaller as the failed glass panel will absorb part of the blast wave's energy. However, the pressure may eventually be larger as the blast wave is reflected by multiple surfaces at the internal of the building. Usually the blast wave cannot flow freely through a building's interior, since it is obstructed by the wall partitions. The pressures due to the propagation of the blast wave through the building load the roof, the side and rear walls directed toward the outer environment, whereas the pressures on the external surfaces are directed towards the interior of the building. This means that the two loads (internal and external) have opposite directions. If the response of the overall structure is evaluated, the loads at the structure's interior can be neglected. However, if the motion of specific components is of interest, the combined loading effect of the internal and external pressures should be considered (taking into account the time delay as a result of the glass panel failure). The internal pressures should be added to the ones produced from the negative phase of the pressure-time history at the outer surface of the structural elements, as described in (Kingery and Bulmash, 1984).

At the current guideline, no further analysis is performed concerning the influence of openings on structures loaded through blast induced loads. In the majority of cases, the pressure and impulse values of the positive phase of a blast pressure-time history are higher than the ones produced from the combined effect of the negative phase at the outer surface and the pressures acting on the interior faces after the failure of the windows.

### 3.7.6 Damage definition

One of the most commonly used tools for assessing the produced damage in a structural member under blast-induced loads are the pressure-impulse (P-I) diagrams. These diagrams, also known as iso-damage curves, are used for calculating the response of a particular structure under a specific load type (e.g. pressure). The P-I curve represents the critical combination of positive impulse-peak pressure for a determined damage level (displacement, rotation etc.). Fig. 22 shows a typical P-I threshold curve and the influence of the structure's fundamental period on its response. In detail, as was proved by Baker (Baker et al. 1983), if the positive duration of the excitation  $t_0$  is significantly longer than the natural period of the structure  $T_n$  ( $\omega_n t_0 > 40$ ), as often the case in seismic loading, the response of the structure is sensitive to the maximum pressure value, as the maximum deflection takes place before the excitation ceases, where  $\omega_n$  is the structure's natural frequency. If the duration of the excitation is much lower than the natural period of the structure ( $\omega_n t_0 < 0.4$ ), the structural response is sensitive to the associated impulse. The behaviour of the structure at the region located between these two extremes is more complex, as it is influenced by both the applied pressure and impulse. Usually, the majority of the structures has a natural period far greater than the duration of a blast positive phase (which is in the order of milliseconds), so they are loaded according the impulse value of the wave time history. By considering rigidity of the structure throughout the passing of the blast wave, the analysis can be performed as decoupled, meaning that the structural response is calculated without allowing for any interaction between the blast pressure loading and the deforming structure.

**Figure 22.** Sketch of a typical Pressure-Impulse diagram.



For creating a P-I diagram, the definition of a damage level or of a maximum displacement limit is a prerequisite. Damage levels for the case of blast loads do not necessarily agree with those established for other load types, e.g. earthquake loading. Even though certain features of seismic design may also be desired in the case of blast loading (ductility, load redistribution etc.), an explosion may result in local failures that were not foreseen during the damage level characterization for seismic loads. Typically, damage levels for explosions are not correlated to the member's stress level, as yielding is usually not excluded to grant economic design. Instead, deformation criteria are utilized, that incorporate the concept of acceptable damage. The proposed deflection limits exclude total or partial structure collapse and classify damage into repairable and unreparable. Damage levels are associated to certain protection levels, as has been described in (UFC-3-342-02, 2008 and ASCE 1997, ASCE 2011). The definition and number of protection levels (and accordingly damage levels) among the different manuals is not unified, which makes the comparison of P-I diagrams complicated.

The deformation parameters that are commonly used as criteria for specifying the damage level limits of a structural component are the ductility ratio ( $\mu$ ) and the support rotation ( $\theta$ ). The ductility ratio is defined as the maximum member deflection divided by its yield deflection,

$$\mu = \frac{\delta_{\mu}}{\delta_y} \quad (4)$$

where:

$\delta_{\mu}$  is the maximum member deflection, and

$\delta_y$  is the deflection under which the member starts yielding.

Similarly, the support rotation ( $\theta$ ) of a member is defined as the angle formed at the support between the member at its maximum deflection and its initial position,

$$\theta = \arctan\left(\frac{x_m}{d}\right) \quad (5)$$

where:

$x_m$  is the maximum member deflection, and

$d$  is the distance from the point of maximum deflection to the support.

The ductility ratio and support rotation values have been used extensively in design manuals to quantify the damage level in a structural member and to produce P-I curves. Their connection to a component's damage state is performed through the introduction of certain limits that have been calculated based on different experimental databases. The proposed values reflect the specific demands, conservatism and priorities of each issuing authority, so a direct comparison among them could lead to misleading conclusions.

Table 5 shows the damage limits and response criteria proposed from the 'Blast Protection of Buildings' (ASCE, 2011) design manual issued by the American Society of Civil Engineers and addresses 12 structural component types. It introduces four protection categories (very low, low, medium and high) each associated with certain performance goals and potential degree of damage to the relevant elements. The element damage is described as superficial, moderate, heavy and hazardous (no visible damage, small repairable permanent deflections, significant unreparable permanent deflections and imminent failure respectively). As with other blast manuals (UFC 3-340-02, 2008 and ASCE, 1997), the proposed limits have been quantified from both dynamic experimental data and static tests. Clearly, the criteria developed through static experiments are more conservative than those from actual blast tests, as several mechanisms are neglected (dynamic material properties etc.). The proposed limits from other blast design manuals (UFC 3-340-02, 2008 and ASCE, 1997) can be also utilized, bearing in mind that the number of protection categories is smaller.



**Table 5.** Deformation criteria for blast-induced elements (modified from ASCE, 2011).

Component type	Expected element damage							
	Superficial		Moderate		Heavy		Hazardous	
	$\mu_{max}$	$\theta_{max}$ $\chi$	$\mu_{max}$	$\theta_{max}$	$\mu_{max}$	$\theta_{max}$	$\mu_{max}$	$\theta_{max}$
<b>Reinforced Concrete</b>								
Single-reinforced slab or beam	1	-	-	2°	-	5°	-	10°
Double-reinforced slab or beam (without shear reinforcement)	1	-	-	2°	-	5°	-	10°
Double-reinforced slab or beam (with shear reinforcement)	1	-	-	4°	-	6°	-	10°
<b>Prestressed Concrete</b>								
Slab or beam with $\omega_p > 0.30$	0.7	-	0.8	-	0.9	-	1	-
Slab or beam with $0.15 \leq \omega_p \leq 0.30$	0.8	-	0.25/ $\omega_p$	1°	0.29/ $\omega_p$	1.5°	0.33/ $\omega_p$	2°
Slab or beam with $\omega_p \leq 0.15$ (without shear reinforcement)	0.8	-	0.25/ $\omega_p$	1°	0.29/ $\omega_p$	1.5°	0.33/ $\omega_p$	2°
Slab or beam with $\omega_p \leq 0.15$ (with shear reinforcement)	1	-	-	1°	-	2°	-	3°
<b>Masonry</b>								
Unreinforced	1	-	-	1.5°	-	4°	-	8°
Reinforced	1	-	-	2°	-	8°	-	15°
<b>Structural Steel</b>								
Beam with compact section	1	-	3	3°	12	10°	25	20°
Beam with non-compact section	0.7	-	0.85	3°	1	-	1.2	-
Plate bent about weak axis	4	1°	8	2°	20	6°	40	12°
<b>Open Web Steel Joist</b>								
Downward loading	1	-	-	3°	-	6°	-	10°
Upward loading	1	-	1.5	-	2	-	3	-
Shear response	0.7	-	0.8	-	0.9	-	1	-
<b>Cold-formed Steel</b>								
Girt or purlin	1	-	-	3°	-	10°	-	20°
Stud with sliding connection at top	0.5	-	0.8	-	0.9	-	1	-
Stud connected at top and bottom	0.5	-	1	-	2	-	3	-
Stud with tension membrane	0.5	-	1	0.5°	2	2°	5	5°
Corrugated panel (1-way) with full tension membrane	1	-	3	3°	6	6°	10	12°
Corrugated panel (1-way) with some tension membrane	1	-	-	1°	-	4°	-	8°
Corrugated panel (1-way) with limited tension membrane	1	-	1.8	1.3°	3	2°	6	4°
<b>Wood</b>								
	1	-	2	-	3	-	4	-
<b>Glazing System Framing</b>								
Aluminum	1	-	5	3°	7	6°	10	10°
Steel	1	-	-	3°	-	6°	-	10°

### 3.8 Protective measures against explosive loads

#### 3.8.1 Façade protection

The adoption of glass façades in the construction of commercial buildings and office complexes is part of an emerging architectural trend that aims at bringing more transparency and daylight into a building's core. It is therefore not surprising that many manufacturers claim an excellent all-glass façade performance under

extreme weather conditions, failing though to consider its response during an explosive event. In case of an external explosion, the building's façade is the first component that has to withstand the produced blast wave, and since glass is one of the most fragile parts of a building due to its low tensile strength, care should be taken to avoid the formation of splinters that could prove lethal due to their high velocity.

Blast-induced injuries may be immediately observable, such as blunt and penetrating traumas due to flying debris and body impact, while others may be initially occult and have a delayed onset of manifestation caused by complex interactions of the blast wave with the body tissues. Traditionally, four basic mechanisms of blast injury are distinguished, which are termed as primary, secondary, tertiary and quaternary (Solomos et al., 2020). The primary mechanism refers to the interaction of the blast wave with the body and the transmission of the external force from the body surface to the internals, the secondary regards injuries caused by fragments of the detonating device or by the generated flying debris, the tertiary includes injuries due to the displacement of the whole body by the blast wind and its subsequent tumbling and sliding on rough surfaces and the quaternary mechanism refers to all injuries, illnesses or disturbances due to exposure to explosions that not fall in the previous three categories.

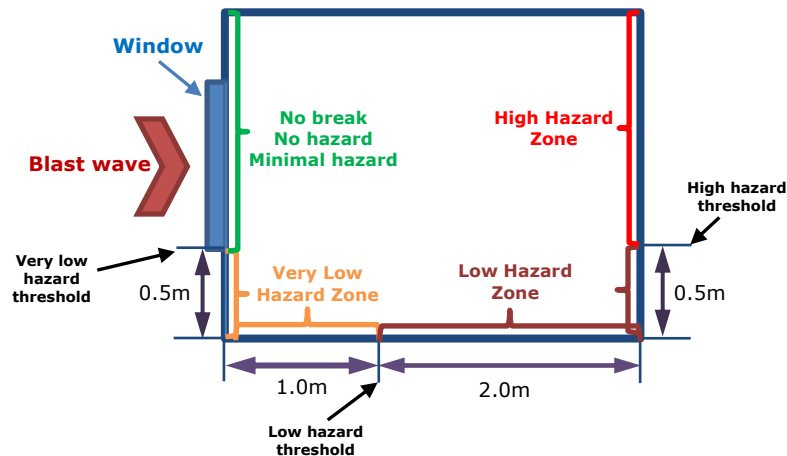
Findings from prior intentional and accidental explosion incidents (Oklahoma city bombing 1986, Jakarta bombing 2004, Cyprus naval base explosion 2011, Brussels airport 2016 etc.) revealed that shattered windows spanned several hundreds of meters away from the detonation point. Window fragmentation is a phenomenon associated with several victims and a great number of injuries, as the fast travelling splinters may easily penetrate the human body. However, by focusing only on the generation of splinters, we fail to notice other important injury mechanisms, such as those related with the produced structural debris (secondary blast injuries either from the window's frame or from the room's interior) and the propagation of the blast through the building (primary blast injuries). It can therefore be deduced that the construction of window elements with increased resistance against explosions or the introduction of splinter arresting mechanisms may lead to the minimization of direct and indirect glass shattering-related injuries and casualties.

The behaviour of glass as a material depends heavily on its manufacturing process and its chemical composition. In most cases, monolithic window-glass types are characterized by large failure strength variations due to the presence of micro-flaws that are invisible to the human eye. The compressive strength of window glass is much higher than its tensile strength and can be classified taking into account its production method, as shown accordingly:

- **Annealed glass (AN):** It is one of the most economic solutions and is produced by being cooled at a slow, moderated rate. Its low tensile strength (nominal value: 45MPa) makes it suitable for window frames at installations without heightened security needs or without people presence.
- **Heat-Strengthened glass (HS):** Its tensile strength (nominal value:70MPa) is higher than the previous glass type as a result of its production technique, as it undergoes a specialized heating and cooling process that induces surface compression (residual stresses).
- **Fully Tempered or Toughened glass (FT):** The manufacturing process is similar to that of the HS glass, but higher temperature ranges are used. After production, both surfaces of the glass pane remain under compressive residual stresses, which means that the flexural tensile strength of the FT glass is higher than the AN glass and strength variation is smaller. The induced tensile stresses from a blast wave, have to overcome the existing compressive stresses. Additionally, in case of failure, the produced fragments are smaller and smoother, resulting in smaller injury risk.

The performance of glass under explosive loads has been examined by various researchers over the last decades. Private companies have also tested specific commercial solutions to validate their efficiency so as to be used in security applications. Since most glass panes will fail when facing a blast wave, many technical guidance documents and codes provide threat ratings associated with the distance travelled by the created glass fragments. For instance, ISO 16933 (ISO16933, 2007) and ASTM F1642 (ASTM1642M assigns a very low hazard rating to fractured glazing whose significant parts are located up to 1m from their original location, whereas a low hazard is designated when these parts lie between 1m and 3m from the original location of the pane's rear face as illustrated in Fig. 23. Similar ratings exist in other documents, such as the GSA TS01 (GSA, 2003) and the ASTM F1642 (ASTM, 2017) test standards, but as noted in the findings of the ERNCIP thematic group (Bedon et al. 2015 and Arrigoni et al. 2017) they are only applicable to specific window geometries, while the velocity, shape and size of the produced fragments is not considered in the definition of the hazard ratings.

**Figure 23.** Glass ratings under arena testing (modified from ISO 16933 and ASTM F1642M).



Blast experiments of the above-mentioned glass types, revealed that a fragment's size, velocity and distance covered after an explosion depend on the produced reflected overpressure and reflected impulse. The fact that the developed fragments pose a significant danger for building occupants, led to the creation of solutions that ensure an increased protection in case of an external explosion. The increased cost of protective measures calls for a clear, case-specific, scenario-based risk assessment process that can reveal the required protection level in order to avoid oversized, expensive solutions. Designing a building façade for resisting an explosive load may prove unfeasible in both economic and practical terms; though lighter measures may be adopted that are capable of mitigating the effects of glass breakage, such as number and velocity of fragments, and consequently number of victims and glass laceration injuries. Over the last years many methods have been developed for minimizing these consequences, the most popular of which are described below:

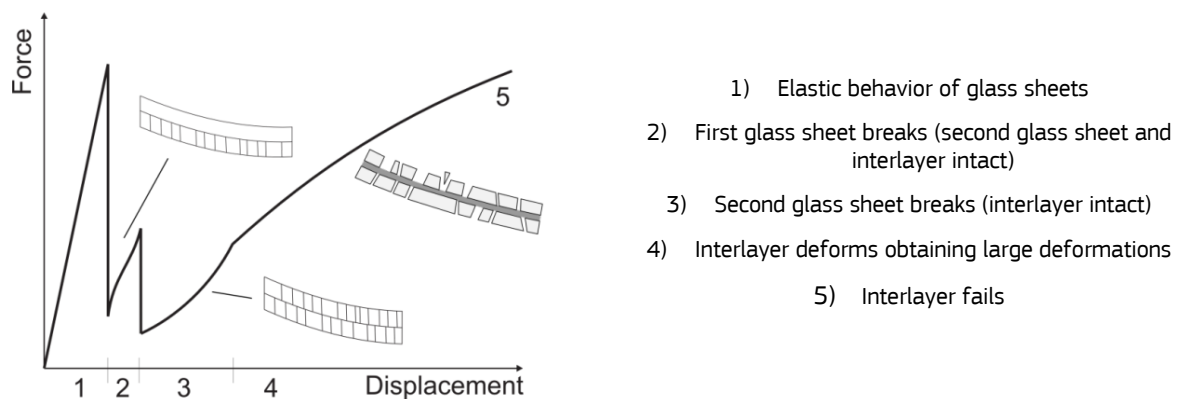
### **3.8.1.1 Anti-shatter films (ASF)**

The installation of ASF is one of the most economical and easiest methods for upgrading the security characteristics of existing window glazing. ASF are composed from a single or multiple polyethylene films that are affixed to the glass through an adhesive. During a blast, the ASF is capable of holding together the produced glass splinters and minimize the risk from fragment-related injuries. Their protection capabilities depend on a number of factors, including, but not limited to, the adhesive component, the glass type, the window size and the strength, thickness and ductility of the film. Moreover, their effectiveness when facing a shock wave is significantly influenced by the employed application methodology. They are usually installed by the so-called "daylight application", which means that the film is applied at the interior of the glass and its size fits the one of the window frame (some millimetres difference appear at the window's edges for installation purposes). This application might result in the entire glass sheet flying at high speed at the interior of the building as a single object, as the blast generated fragments are held together by the film. Alternatively, the ASF may be wrapped around the edges of the glass, but that requires the removal of the glass from its frame, a procedure that is both time consuming and demanding. Specialized anchoring systems that are fixed to the window frame (as long as it is strong) may also be used for holding the filmed glass in place after its failure. ASF are available in different thicknesses, and depending on the intended use, thicker options may be adopted for exterior and/or larger windows with small stand-off distances. If possible, ASF should be installed as a single piece avoiding large edge distances (for daylight applications) from the window frame. Their impact capabilities and classification are controlled through the EN12600 (EN12600, 2002), while the performance of the adhesive can be assessed through a peel test as proposed by CPNI (CPNI EBP 10/13). Apart from the protection in case of blasts, ASF are also effective against intrusion attempts by the use of sharp objects and are typically equipped with UV protection characteristics. However, it is highlighted that ASF are efficient only for relatively large scaled distances and should be considered as part of a holistic security plan and not a stand-alone solution. Despite being an economical solution for retrofitting existing façades, films are not protected by two glass layers like in laminated glass and are exposed to the environmental conditions that resulting in ageing of their material. Their exposure makes them also vulnerable to scratches, chemical agents and heat, since they are much less resistant than glass. Their substitution is an expensive and complicated process, especially if they are wrapped around the edges of the glass.

### 3.8.1.2 Laminated glass

Laminated glass is widely used for mitigating the consequences of an explosion in building facades, and is composed of two or more glass sheets that are separated by polymer inter-layers, such as polyvinyl-butylal (PVB), ionoplast polymers and ethylene-vinyl acetate (EVA). The advantage of laminated glass is its ability to hold together the created glass fragments (they remain stuck to the interlayers) and dissipate the blast energy though its elevated ductility. Fig. 24 shows graphically the failure mechanism of a laminated glass pane with one interlayer (Larcher et al. 2012). As observed in the figure, in the first stage of its failure mode, laminated glass responds as an elastic plate, similar to a monolithic pane. However, after fracture of the glass sheets, fragments are glued to the interlayer and the laminated glass behaves as a membrane, failing when the interlayer bonding material tears.

**Figure 24.** Failure mechanism of laminated glass.



By using multiple (and thicker) glass panes and interlayers, the strength of the window increases, as in the case of bullet-resistant glass. The use of laminated glass as a retrofitting solution needs to be combined with strengthening of the surrounding window frame that has to transfer the produced reaction forces at the building’s frame. This means that in the design, the window frame and its connections has to fail at a later stage than the laminated glass to prevent failure of the glazing system that could cause injuries if it detaches from its supporting wall. If the pressures to be sustained by the window system are high, the frame can be anchored to the surrounding wall by means of steel bars, cables or steel plates. Special attention is also required at the window depth that is captured by the frame (minimum recommended depth equal to 1.5cm) and the amount of sealant that is used.

There exist different standards for the classification of laminated security glass depending on the attack that has to be mitigated, such as ballistic, manual or explosive. Classification is provided after physical testing that corresponds to the mitigation needs, meaning pendulum tests for glass impact (EN12600:2002), steel ball tests for manual attack (EN356:1999), ballistic tests for bullet proof glazing (EN1063:1999) and blast tests [shock tube (EN13123-1:2004) or arena testing (EN13123-2:2004)] for explosion resistance (EN13541:2012).

Table 6 shows the glazing classes quantifying the performance under impact and providing insight at the breakage modes. Testing is performed by a pendulum using a 50kg impactor that is released from different heights and can cause three modes of breakage (type A, B or C) differentiating in the number and size of produced glass fragments.

**Table 6.** Classification for glazing resistance to impact.

Attack type	Standard	Classification	Breakage mode	Drop height (mm)
Glass impact	EN 12600	3	A, B, C	190
		2	A, B, C	450
		1	A, B, C	1200

Table 7 presents the classification of glazing that has to be resistant against manual attacks. The test consists of a steel sphere (4.11kg) that impacts the examined glass dropped from different heights (classes P1A-P5A) and a swinging axe test for the rest of the classes (P6A-P8A).

**Table 7.** Classification for glazing resistance to manual attacks.

Attack type	Standard	Classification	Drop height (mm)	No of axe strikes
Manual attack	EN356	P1A	1500	3 (in a triangle)
		P2A	3000	3 (in a triangle)
		P3A	6000	3 (in a triangle)
		P4A	9000	3 (in a triangle)
		P5A	9000	3x3 (in a triangle)
		P6A	-	30-50
		P7A	-	51-70
		P8A	-	>70

The performance of bullet resistant glazing is quantified through a series of tests with different weapons (rifles, handguns or shotguns) corresponding to the desired protection level. The class is obtained if the examined glass has not been penetrated by the number of fired shots. An additional rating exists to indicate whether splinters have been produced (S) or not (NS).

**Table 8.** Classification for glazing resistance to armed attacks.

Attack type	Standard	Classification	Caliber	No of shots	Bullet velocity (m/s)	Test range (m)
Armed attack	EN1063	BR1-S (NS)	0.22 LR (rifle)	3	360	10
		BR2-S (NS)	9mm Luger (handgun)	3	400	5
		BR3-S (NS)	0.357 Magnum (handgun)	3	430	5
		BR4-S (NS)	0.44 Rem. Magnum (handgun)	3	440	5
		BR5-S (NS)	5.56x45 (rifle)	3	950	10
		BR6-S (NS)	7.62x51 (rifle)	3	830	10
		BR7-S (NS)	7.62x51 (rifle)	3	820	10
		SG1-S (NS)	12/70 (shotgun)	1	420	10
		SG2-S (NS)	12/70 (shotgun)	3	420	10

Table 9 shows the test conditions for the assessment of explosion resistant glazing for use in buildings that offer increased human safety against explosives. The tested glass sizes are approximately 1m<sup>2</sup> (1.1mx0.9m) and can be tested using a shock tube or a similar device that can produce a plane shock wave, normal to the clamped specimen, with the characteristics described in Table 9.

**Table 9.** Classification for glazing resistance to explosive attacks.

Attack type	Standard	Classification	Maximum reflected overpressure (kPa)	Positive reflected impulse (kPa·ms)
Attack with explosives (glazing)	EN13541	ER1	$50 \leq P_r \leq 100$	$370 \leq i_{r+} \leq 900$
		ER2	$100 \leq P_r \leq 150$	$900 \leq i_{r+} \leq 1500$
		ER3	$150 \leq P_r \leq 200$	$1500 \leq i_{r+} \leq 2200$
		ER4	$200 \leq P_r \leq 250$	$2200 \leq i_{r+} \leq 3200$

Table 9 describes the classification requirements only for explosion resistant glazing. Though, the resistance of the entire window system against explosions is also of interest to avoid it from being propelled into the building. A specialized classification has been established by employing an experimental procedure through the use of shock tubes (EN13123-1: 2004) or arena tests (EN 13123-2: 2004). Table 10 presents the classification for window systems in order of increasing resistance for both test methods.

**Table 10.** Classification for window system resistance to explosive attacks.

Attack type	Standard	Classification	Maximum reflected overpressure (kPa)	Positive reflected impulse (kPa·ms)
Attack with explosives (window system)	EN13123-1	EPR1	$P_r \leq 50$	$i_{r+} \leq 370$
		EPR2	$50 \leq P_r \leq 100$	$370 \leq i_{r+} \leq 900$
		EPR3	$100 \leq P_r \leq 150$	$900 \leq i_{r+} \leq 1500$
		EPR4	$150 \leq P_r \leq 200$	$1500 \leq i_{r+} \leq 2200$
	<b>Standard</b>	<b>Classification</b>	<b>Charge mass (kg)</b>	<b>Stand-off distance (m)</b>
	EN13123-2	EXR1	3	5.0
		EXR2	3	3.0
		EXR3	12	5.5
		EXR4	12	4.0
		EXR5	20	4.0

### 3.8.1.3 Catching systems

**Bars/cables/anchoring systems:** The application of bars is usually combined with the use of anti-shatter films or laminated glasses, as an additional mitigation measure. These catcher bars are anchored at the interior

of the window frame and positioned horizontally and/or vertically in order to stop the glazing from flying into the building, should it fail. Solutions with only one bar positioned at the opening's mid-point are also available so that the failed glazing wraps around the bar when it is projected into the room. A key point in the design of such bars is their anchoring to the window frame, that needs to be firm enough to sustain the forces that are created due to the failure of the glazing system. Flexible systems and energy absorbing cable solutions are also available in the market and they are designed to absorb part of the energy that is transmitted to the system after the impact of the blast wave. Cable systems due to their flexibility can be fitted to different window geometries, while they may be combined with shock absorbing devices to increase the system's energy absorbing capacity. Such devices may be considered in case of relatively weak window frames, as part of the blast energy that would be absorbed entirely from the frame (in case of rigid connections) can be absorbed by the installed device. During the design phase and depending on the considered blast scenario, the cables' diameter, their fixings and their spacing are parameters that need to be calculated.

**Curtains/nets/membranes:** These catching systems are stand-alone structures or coupled with the use of anti-shatter films or laminated protective glass solutions. Their main aim is to catch the flying fragments that are produced from the failure of the windows as a result of a propagating blast wave and they are usually installed behind the building's façade. Clearly, their anchorage to the window frame needs to be properly designed to avoid failure of the system. In detail, blast curtains are generally manufactured from ductile polyester materials and are fixed only at the top of the opening. This type of installation guarantees adequate venting of the blast wave as it is not mounted at the sides or the sill of the window, while it successfully captures the created glass splinters. Such protective drapes need to be left in their original position, as if they are pushed aside from the building occupants, they lose their mitigation capacity. Nets are made of steel or polyester ropes that are usually anchored at the entire perimeter of the window frame. They can be very effective in retaining larger glass parts, but their performance is usually poor if glass splinters are produced, which indicates that they should be coupled with an anti-shatter film installation.

Both systems are mainly used in case of very high security demands since their installation results in the reduction of the window transparency and might not be accepted in case of moderate risk level.

#### **3.8.1.4 Supporting walls**

The surrounding walls of a structure are usually overlooked during a blast assessment, as they are considered to be able to withstand the produced blast wave. Though this is true for the majority of cases, special attention is required for weak, unreinforced masonry walls that may fail under large explosions. To guarantee that after an explosion windows will fail first, the supporting walls need to be at least as strong as the window systems. This can be performed through the application of an interior (and potentially exterior) polymer coating or the retrofitting of a geotextile fabric that may contain the produced wall fragments due to their ductile nature and deformation capabilities. This means that the aim of these techniques is not the strengthening of the wall itself but the confinement of the produced fragments. Alternatively, the window frames may be directly anchored to the concrete slabs or the building's perimeter beams (spandrel beams), so that the resulting reaction forces do not have to be sustained by the masonry walls.

#### **3.8.1.5 Contact detonations**

As highlighted before, the proposed blast parameters in Fig. 13-16 should be treated with caution at small scaled distances, as the phenomena following close-in detonations include big uncertainties. This is the case if the IED is placed very close or in contact to a structural element, such as a load-bearing column or wall elements that are more critical as they can trigger a progressive collapse mechanism. For determining the consequences of near-field detonations, complex fluid-structure numerical simulations are usually employed, especially if failure of the examined element could result in the partial or progressive collapse of the supported structure.

Designing new or existing structures to sustain an explosion may include the strengthening of structural elements at locations deemed as vulnerable. These locations are usually accessible by the public, such as the ground floor of a facility or the underground garage levels, and are considered potential areas for the placement of an IED. An easily applicable technique is to embed the structural elements at the locations of interest in high performance concrete and increase their dimensions, especially in case of contact detonations. The additional concrete layer will protect the embedded structural elements and only act as an 'absorber' in case of an explosion, without contributing to their axial capacity. Moreover, due to the increased concrete layer, the scaled distance of the explosive from the load-bearing element increases. Other similar flexible, non-intrusive and cost-effective techniques are the strengthening of the structural members by the use of glass, steel or carbon fibre reinforced polymer composites (Berger et al. 2008, Vapper et al. 2020). Clearly, the most effective

technique is the increase of the scaled distance, and therefore decrease the severity of the damage to the structural element, accomplished either by limiting the free access to the public or by adopting measures that prohibit a charge from being directly in contact to a load bearing member, e.g. by encasing a column in isolating material. However, the increase of the scaled off distance is not always possible, so strengthening of the structural elements may be required by adopting one of the above-mentioned techniques.

### **3.8.2 Access control zones**

In response to the heightened terror threat in recent years, an increasing interest is observed in the introduction of access control zones at critical infrastructures and sites that have an increased likelihood of being the target of a terrorist attack. To ensure that the relevant threats remain outside the main core of the buildings, these areas are tailored for screening visitors and personnel through the installation of appropriate electronic access control systems. Such control zones are characterized by people congregation, while they are usually located either at the interior of the site/building that has to be protected or directly attached to it. Clearly, the best solution in terms of security is the creation of the control zone in a structure that is separate from the main building, though the increased space requirements are often prohibitive, especially in city centres, and visitors would have to exit the control zone after screening in order to enter the main building, which makes them vulnerable to inclement weather. The elevated security needs in these areas call for a design that has to consider the risk of internal explosive events and identify appropriate strategies that can effectively limit the consequences of an internal blast, while guaranteeing that the created blast wave will not propagate into the vulnerable, secured areas of the facility.

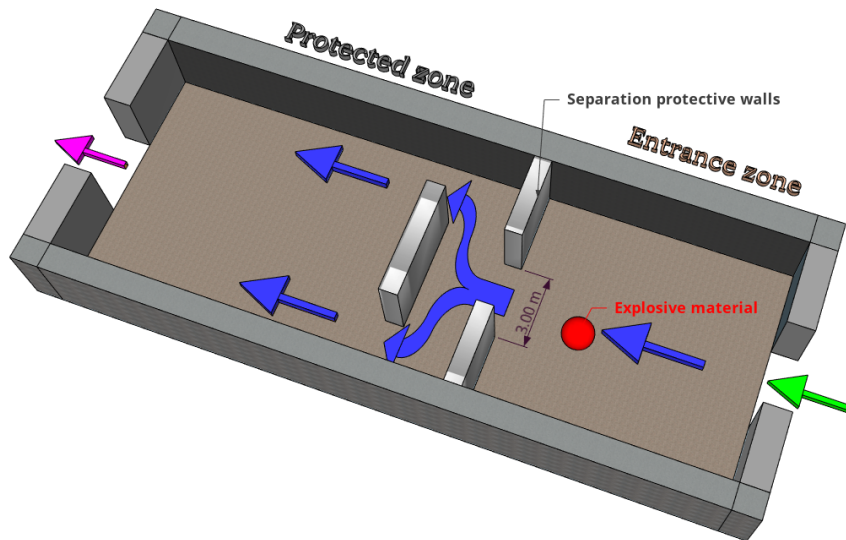
The detonation of explosives at a building's interior leads to complicated pressure patterns, due to the reflections of the produced blast wave on the surrounding walls and objects. Due to the complexity of the phenomenon, numerical simulations or experiments are employed to calculate the pressures that are applied to the various structural and non-structural components. The consequences of an interior blast depend not only on the charge weight and its detonation centre, but also on the shape, the dimensions and the venting characteristics of the space where the explosion occurs. The design of access control zones needs to be resistant from both internal and to a certain extend also from external explosions, while avoiding creating additional vulnerabilities, like the creation of bottlenecks and queuing in front of the building's entrance. The following physical protection measures may be adopted to limit the effects of an explosion in an enclosed environment.

#### **3.8.2.1 Separation protective walls**

The geometric features of an access control zone significantly affect the propagation of the produced blast wave. The reflections of the blast wave on the existing walls, the ground, the ceiling and other objects may result in either shielding certain areas or focusing the propagating shock wave, influencing exposed persons or structures. For understanding the complexity of these phenomena, powerful numerical tools are available that employ sophisticated fluid simulations or even fluid-structure interaction techniques to predict the behaviour of blast waves into a complex enclosure. The geometry of such a numerical model is shown in Fig. 25, where an entrance zone, located on the right, is connected to the protected zone on the left through a series of blocking walls that leave a 3m-wide opening. These separation walls form a barrier between the explosive material located in the entrance zone and the vulnerable area on the left, protecting it both from the blast wave and the flying fragments that may be produced due to the detonation of the IED.



**Figure 25.** Protective blast walls.

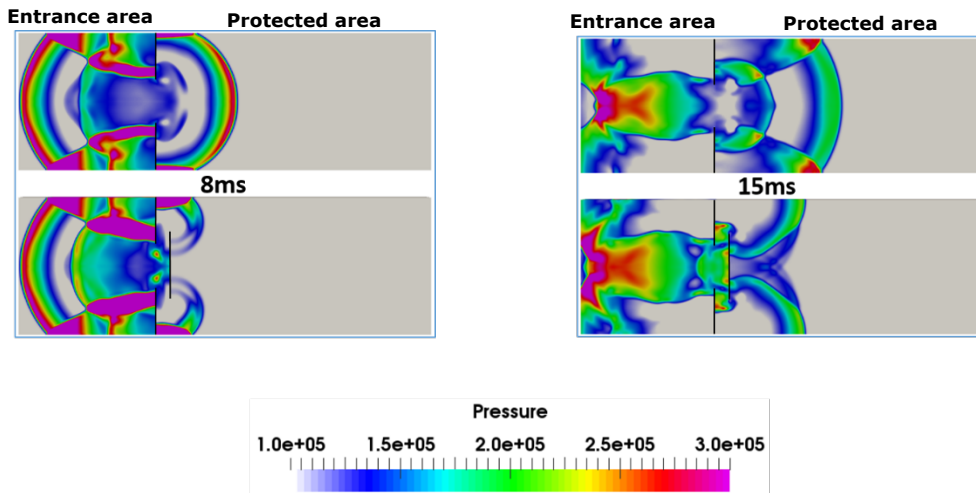


These separation walls need to be hardened by the use of appropriate reinforcement and rigid connections to resist the results of an explosion without failing or with minimal damage. They serve mainly in reflecting the blast wave back into the entrance zone and therefore protecting the part of the building that is considered more vulnerable. Minimizing the propagation of blast pressures within a building is crucial, due to their destructive consequences to structural and non-structural elements, and their life-threatening effects against the facility occupants (lung haemorrhage, eardrum rupture, inhalation of smoke and dust, trauma from furniture and building elements etc.).

The construction materials of the separation walls have a strong influence on their performance under the impacting blast load or potential impact of fragments and projectiles. Popular material options include, but not limited to, poured-in or precast concrete, reinforced concrete masonry units, metal sheets and bullet-proof laminated glasses. These walls, depending on their material and the scaled distance of the explosives, might undergo permanent deformations and absorb only part of the created blast energy. This means that a combination of blast wave reflection and energy absorption can potentially take place. Care should be provided though, so that an eventual failure of the separating walls does not produce fragments that could lead to injuries. Usually, IEDs that may be placed by an aggressor in welcome centres and similar confined spaces (person borne IEDs) are much smaller than the IEDs considered in open spaces when a vehicle borne IED is examined. Consequently, the blast walls that are required for protection against internal explosions are usually much smaller in size and have lower resistance to blast pressures and impulses than the ones designed when explosions outside the building are examined.

Blast separation walls are usually robust enough to not sustain significant damage in case of an explosion, as they are rigid, massive structures. Still, weaker systems can offer a certain degree of protection (as long as they do not produce potentially lethal fragments) and their significant deformation is a manifestation of a blast energy absorption mechanism. Shear walls (concrete, steel or reinforced masonry) that are commonly used in various buildings as part of the load bearing system, can also be used as separation blast walls, as long as their potential failure will not generate a progressive collapse of the structure. Fig. 26 shows the pressure distribution of a blast wave at 8ms and 15ms after the detonation of 25kg of TNT, located at the entrance area of the access control zone demonstrated in Fig. 25. The two different models that are compared display the behaviour of the blast wave when the separation rigid blast wall is in place ('meandering' case) and when it is missing ('open door' case). It is observed that when the wall is present there is a significant reduction in pressure values at the 'protected area', mitigating to a great extent the consequences of the explosion that occurred in the 'entrance area'.

**Figure 26.** Blast wave pressure distribution [Pa] for the ‘open door’ case (upper images) and the ‘meandering’ case (lower images) at 4ms and 10ms after detonation.



The additional separation wall reflects part of the initial blast wave and guides it back to the entrance area, resulting in slightly higher pressures into this zone. Since the entrance area has already been significantly affected by the initial blast wave, the additional energy due to the reflection on the separation wall does not affect the injury risk probability. This analysis demonstrates that such a design can be effectively adopted to isolate access control points from attached buildings when a terrorist attack scenario at the structure’s interior is considered. As a result, the introduction of separation walls reduces the consequences of the propagating blast wave, limit the dispersion of potential fragments contained in the explosive device and offer enhanced protection from shooting attacks.

An additional security measure is the introduction of revolving doors between the control zone and the rest of the building (if they are connected), in order to mitigate the consequences from an active shooter incident. Access through these doors may be granted through a magnetic card or other similar system and they can be locked in case of an attack. This additional measure acts as an obstacle and reduces the propagation speed of the armed aggressor, providing security forces more time to react.

### 3.8.2.2 Explosion venting

In the majority of cases, confined explosions are more severe than external, open-air explosions of the same explosive, as the multiple reflections of the blast wave, the detonation products and the afterburning effect of the flammable gases result to pressure distributions with a greater number of peaks and longer durations, which translates to much higher impulse values. Venting openings serve for releasing the created blast wave in the surroundings of the facility and effectively reducing the pressures build-up (both their magnitude and duration) at the interior of the area under consideration. This is a valuable system for reducing the explosive forces in crowded spaces and prevent the blast wave from propagating into adjacent critical facilities. Ideally these venting openings should be uncovered, but for practical reasons they are usually covered by a frangible material (window or blow-out panel type) that opens (or shatters) at a low pressure. Popular types of explosion vents include, but are not limited to:

- Opening covers (relief doors or windows) that open when facing a blast wave
- Panels that are blown out due to the shock front
- Windows from glass that shatter
- Windows from frangible material (membranes or diaphragms) that rupture
- Textile structures

Pressure relief initiates when the explosion-release window systems or blow-out panels are activated, meaning that their pressure limit value is exceeded. They are required to open automatically in a time frame of milliseconds when subjected to an internal pressure (but should resist externally applied pressures), and should be either very light to be easily pushed aside by the created shock front or covered with materials that will instantly fail under high pressure values. Such solutions were initially adopted in combustion plants, solvent

evaporating ovens and explosive dust handling industries to mitigate the results of a potential explosion, by quickly releasing the interior pressures to the surrounding environment and therefore minimizing the reflections on the rest of the structure. The combustion zone propagation velocity in these cases is below the speed of sound (deflagration) making explosion venting more effective in decreasing the developed initial overpressures, whereas in the event of a terrorist attack with explosives the combustion zone propagates (for most explosives) at a velocity greater than the speed of sound (detonation).

The use of fragile glass panels as a cover for the openings located at the perimeter of the building is an effective mitigation measure, but could have a serious negative side effect. Their brittle nature (annealed or tempered glass) can result in the production of flying splinters from the fragmented glass panels that can travel at high velocity affecting a wide area around the building. Their speed is responsible for their high kinetic energy, irrespective of their relatively small masses. Therefore, a fragile glass panel can be dangerous for the personnel and the public located at the exterior of the building in case of an internal blast and should be avoided, unless the surrounding area is not accessible to the public. Thus, such pressure release surfaces are often installed at the roof of the examined structures, as, in case of failure, the impact of the produced fragments is minimized. An alternative way to introduce venting surfaces without the use of glass panes is by adopting ceiling openings covered with lightweight aluminium panels (or similar products, like transparent polycarbonate), which can be released in case of a possible internal explosion. Fig. 27 shows typical examples of explosion release hatches that are available in the market.

**Figure 27.** Typical design of blast release vents.



Blast release vents need to be properly dimensioned, so as to effectively mitigate the results of an internal explosion. Their size depends on a number of elements including, but not limited to:

- The size of the explosive charge
- The type of the explosive charge
- The location of the detonation point
- The geometry and size of the room where the explosion takes place
- The presence of any other venting (e.g. fragile window panes)
- The failure (or opening) pressure of the blast release vent or blow-out panel
- The time required for the activation of the blast release vent or blow-out panel

The majority of blast release vents have been designed to protect an area in the event of deflagration, i.e. an explosion that propagates at subsonic speed. The explosion of high explosive compounds, such as those illustrated in Table 4, moves outward at supersonic speeds, a process known as detonation. Vents designed for deflagration maybe still be effective under detonation conditions, but the high created overpressures might cause permanent damage to their mechanism or their structural integrity. The majority of formulas for the calculation of the required venting area, like those included in (EN 1991-1-7, 2006), (NFPA 68, 2018), (VDI 3673, 2002) and (FM Global 1-44, 2012), have been developed through experimental data of gas and dust explosions, therefore they refer to the design of deflagration vents. Thus, when sizing an explosion vent for a detonation with one of the above-mentioned guidelines, one should bear in mind that its dimensions might be under-designed as the pressures handled by the vent cover might exceed to a great extent those of a deflagration explosion. Still, even if some vent components fail due to the high pressures and are not functional

after the explosion, their purpose of reducing the consequences of an interior blast will have been fulfilled. In order for the lightweight pressure relieving openings to provide minimal resistance to the propagating blast wave they need to be regularly inspected and maintained to guarantee a performance level in line with their initial design.

### 3.8.3 Protection against progressive collapse

Progressive collapse of a structure can be defined as the condition where a local structural failure of one or more primary structural members leads to a chain reaction that results to the disproportional failure and/or collapse (partial or total) of the entire building. This type of failure is usually linked to a great number of injuries and fatalities and can be triggered by a number of causes including, but not limited to, earthquakes, vehicle impacts, design errors and explosions (flammable gas, explosive dust, terrorist attacks etc.). From a security point of view, progressive collapse is of significance to critical infrastructures and other buildings that may face an attack with the use of explosives, such as the terrorist attack against the A. P. Murrah Federal Building in Oklahoma City in 1995 shown in Fig. 28. Designing a structure to resist progressive collapse poses a number of challenges such as determining the size and type of the explosive charge, the location of the detonation point and the building material characteristics under high strain rates. Structural robustness is a key function in the design of structures, as it entails their ability to redistribute the loads from the failed to the intact members.

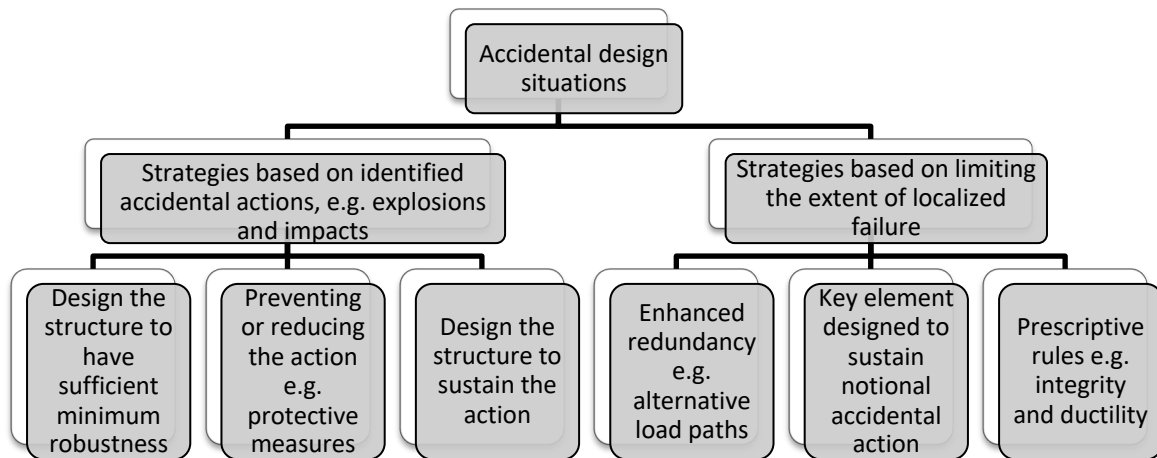
**Figure 28.** Partial collapse of Alfred P. Murrah Federal building [FEMA, 1995].



There exist various methodologies (direct and indirect) for increasing the robustness of a structure to resist progressive collapse, many of which are included in design guidelines and standards mainly from Europe and the USA. The direct design approaches address explicitly the problem of progressive collapse through a performance-based design that aims at reinforcing specific elements to resist the created blast pressure and assess the structure's vulnerability through the Alternative Load Path Analysis method. The indirect approaches do not focus specifically on progressive collapse but bring forward an overall enhancement of building robustness (through minimum requirements on strength, ductility, continuity etc.), irrespective of the loads that might cause collapse.

According to Eurocode EN 1991-1-7 the design of a structure which may face a terrorist attack should be considered an accidental action, as it does not provide specific guidance for actions caused by external explosions, warfare or terrorist activities. Consequence classes are introduced depending on the building types/occupancies and the adoption of the strategies presented in Fig. 29 guarantee that the examined structure has an acceptable level of robustness to sustain localized failure without initiating a progressive collapse mechanism. The acceptable limit of this localized failure in building structures is suggested to be either 100m<sup>2</sup> or 15% of the floor area (whichever is less) on two adjacent floors caused by the removal of a vertical load-carrying element.

**Figure 29.** Strategies for accidental design situations (EN1991-1-7, 2006).



For dedicated rules and provisions for the design of buildings against progressive collapse, one has to resort to American guidelines such as the (GSA, 2013) and (UFC 4-023-03, 2016). The earlier versions of these guidelines only included individual column removal scenarios, comprising of either eliminating a middle column in each of the building sides or a corner column. Depending on the guideline, these scenarios referred to the removal of only the columns located at the ground floor (in the case of the GSA) or the columns located at each floor level (in the case of the UFC). However, their updated versions aim to decrease inconsistencies among the two documents and they both follow a performance-based design approach through the use of the alternate path method. The floor levels and locations from which the vertical load-bearing elements are removed during the analysis (ground floor, underground parking, each floor level, internal/perimeter columns) depend on the security level of the facility. The allowable floor damage limits in the previous versions of the guidelines have been removed and substituted by acceptance criteria and redundancy requirements. An exception is foreseen for existing buildings that are analysed according to the GSA, where a certain amount of local damage is permitted at the floor area adjacent to and directly above the removed element, provided that the falling debris do not cause overloading of the lower floor levels.

The strategies proposed by the above-mentioned standards and guidelines to reduce the likelihood of disproportionate collapse can be summarised as follows:

**Prevention:** A progressive collapse mechanism can be prevented by protecting the examined structure from relevant man-made accidental loads and eliminating or reducing the considered hazard.

**Direct design:** This approach focuses on providing the building structure with adequate resisting mechanisms by either improving the transfer of loads from damaged to intact elements through applying the alternate load path method or by reinforcing key elements that have to withstand the produced accidental loads. For example, critical columns may be protected by embedding them in high performance concrete or by increasing the stand-off distance between the column and the potential IED. The latter may be accomplished by wrapping isolating material around a column.

**Indirect design:** This methodology targets to an overall design that ensures increased ductility and minimum strength through selecting structural forms with low sensitivity to the considered threat, while introducing tying systems to avoid unexpected collapse. Such approaches are already employed in the seismic design of structures aiming at increased robustness.

Table 11 presents the design approaches suggested by three different guidelines (EN 1991-1-7 2006 and GSA, 2013 and UFC 4-023-03, 2016). EN1991-1-7 does not outline exact column removal scenarios but relies on engineering judgement, whereas both American guidelines prescribe specific locations for the removal of

columns or load-bearing walls (interior columns are removed only in case of uncontrolled public access). The different documents agree that only buildings of higher security classes need to undergo such analysis, as their importance, size and people attendance may result in great consequences, should a progressive collapse mechanism be developed. Only EN1991-1-7 sets permissible structural local damage limits at the floors adjacent to the column removal location, while UFC 4-023-03 and GSA introduce acceptance criteria that have to be respected. An exception is made in the GSA for existing buildings, where a localized structural damage at the floor adjacent to the removed column (15% or 30% of the floor area for exterior and interior column removal respectively) is accepted.

**Table 11.** Suggestions during the analysis of structures against progressive collapse according to different standards.

**EN1991-1-7**

Column Removal locations

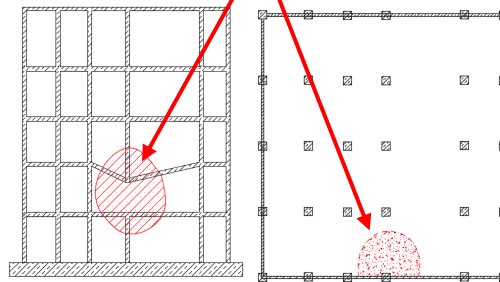
Not specified –engineering judgement

Analysis required for building security classes

(Consequence Class - CC)

CC2b(upper risk group) - CC3

Permitted local damage after column removal  
100m<sup>2</sup> or 15% of floor area in  
two adjacent storeys



**General Services Administration**

Column Removal locations

Analysis required for building security classes (Facility Security Level-FSL)

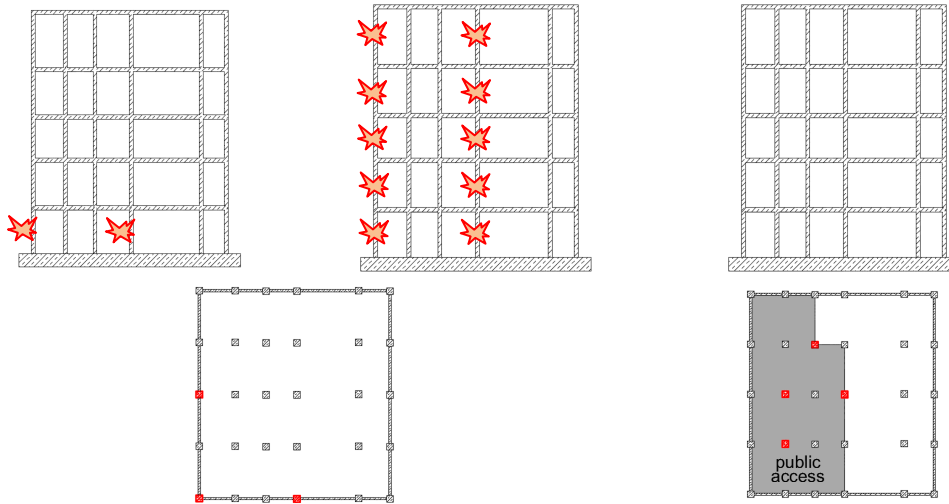
FSL III-IV

FSL V

FSL V

External columns

Internal columns  
(only for underground parking  
and areas of uncontrolled  
public access)



Permitted local damage after column removal

For new  
buildings:  
For existing  
buildings:

Not allowed

<15% of total floor area in the adjacent floors (external column removal)

<30% of total floor area in the adjacent floors (interior column removal)

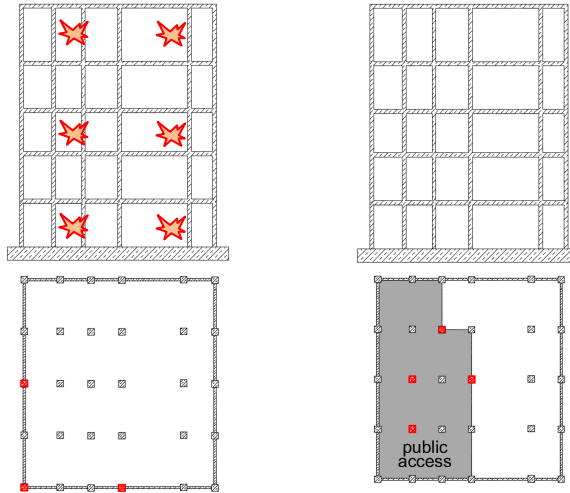
## UFC 4-023-03

### Column Removal locations

External columns

Internal columns  
(only for underground parking and areas of uncontrolled public access)

Analysis required for building security classes  
(Risk category - RC)  
RCII-RCIII-RCIV



Permitted local damage after column removal  
Not allowed

The progressive collapse analysis scenarios that were described in the previous table need to be coupled with the appropriate load combinations during design, as presented in Table 12. It is noted that the updated versions of the two American guidelines have harmonized the load cases that have to be applied and analysed. A load increase factor is recommended in the case of a linear or nonlinear static analysis procedure for the floor areas immediately adjacent to and above the removed column or load-bearing wall. Further information on the value of this load increase factor and the  $\psi$ -factor in the EN1991-1-7 is included in the relevant documents.

**Table 12.** Design load combinations for building progressive collapse analysis.

Guideline	Load combinations	Comment
<b>EN1991-1-7</b>	$G+A_d+\psi Q$	$0 < \psi < 0.9$
<b>GSA/UFC 4-023-03</b>	$1.2G+(0.5L \text{ or } 0.2S)$ $\Omega \cdot [1.2G+(0.5L \text{ or } 0.2S)]$	Valid only for linear/nonlinear static analysis at floors directly above and adjacent to the removed columns

where  $G$ =dead load,  $Q$ =variable load (live load, snow etc.),  $A_d$ =design accidental load,  $\psi$ =factor for variable action,  $L$ =live load,  $S$ =snow load,  $\Omega$ =load increase factor

From the information included herein, it can be deduced that the guidelines existing today still lack more detailed instructions for designing structures against progressive collapse. For instance, in the Eurocodes no specifications are provided concerning the dynamic amplification factor that needs to be employed, when an equivalent static analysis is applied during the design of a building against progressive collapse. More reliable results can be achieved with the use of nonlinear dynamic analysis, that takes into account the various

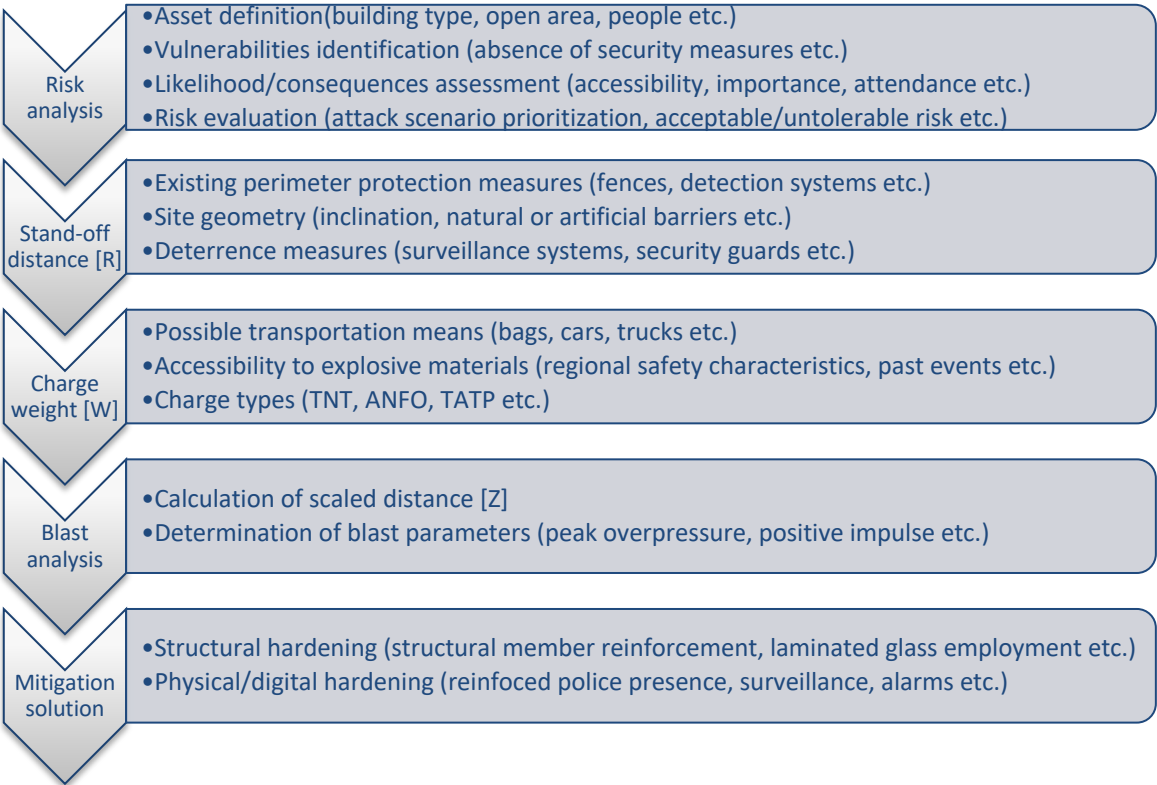


nonlinearities that are present in the phenomenon, or the use of fluid-structure numerical simulations. The design goal is the creation of a structural system that is not sensitive to progressive collapse mechanisms if one or more of its load-bearing elements fail. To accomplish that, an indirect design method may be employed that introduces minimum strength values and tying systems among members, or a direct design method that considers the individual failed elements and the transfer of loads to intact ones. The development of efficient design methods for minimising the likelihood of progressive collapse is essential for modern engineering works, which are often characterized by large spans and specialized loads.

### 3.9 Summary of blast protection design

Blast protection design of a structure against external explosions requires the calculation of the blast loads that have to be sustained by its structural and non-structural components. The most commonly used approach in traditional engineering is based on the empirical and semi-empirical methods that were presented earlier. Though, the formulas, graphs and diagrams that have been included do not cover more complicated cases of blast loading, where obstacles are involved and wave shadowing and channelling phenomena take place. More comprehensive mathematical tools, e.g. explicit finite element codes, need to be employed for calculating the blast parameters, at the expense of added complexity and computational time. Fig. 30 presents an overview of the steps that need to be followed for deciding on appropriate hardening measures against IED attacks.

Figure 30. Blast protective measures design process.



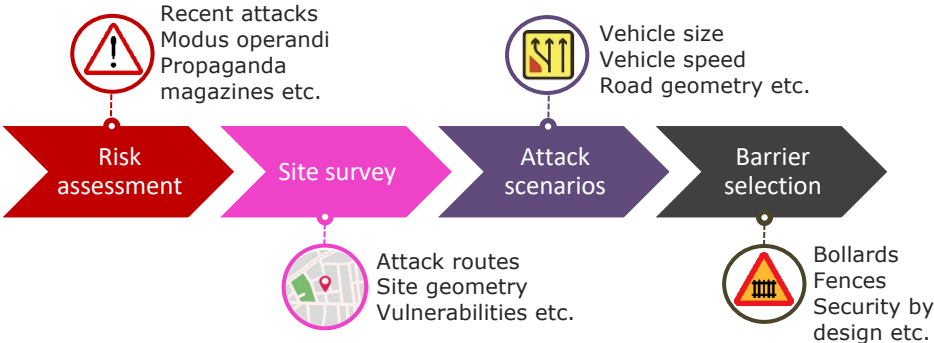
# 4 Protection against attacks with the use of vehicles

## 4.1 General

Terrorist attacks and other malicious acts often target critical infrastructures and public spaces which are characterized by limited protection measures. A tendency has recently appeared to target these unprotected places by means of ramming vehicles that are either deliberately driven at high speed against the public to maximize human casualties or are used for transporting an improvised explosive device (IED) close to a facility. An effective physical perimeter protection strategy of a site aims to minimize the threat of unauthorized vehicle access and set a minimum stand-off distance between the asset to be protected and its perimeter.

Over the last decades, various physical protection measures against unauthorised vehicle access have been developed and applied in public spaces, around buildings and critical infrastructures. Nevertheless, these measures have not always been selected based on a structured approach, designed to take into consideration the unique characteristics of each potential target, but largely depend on practices adopted by the local authorities and the availability of specific solutions. Clearly, traffic rules do not apply to drivers with malevolent intentions, so there is a growing need for designing and implementing an approach that supports the selection of simple, tailor-made and effective perimeter protection measures. This selection procedure can be used by premise owners, building designers, security officials, technical experts or other interested professionals. The proposed framework is graphically demonstrated in Fig. 31.

Figure 31. Selection approach for anti-ramming vehicle barrier selection.



For the purposes of this document, vehicle barriers are devices or other structural obstacles that allow the controlled access of vehicles to an area designated as protected. These barriers should be specifically designed and capable of stopping an ill-intentioned vehicle that attempts to breach the security perimeter. A proper layout of barriers may also be adopted that aims at reducing the speed of threat vehicles to render them incapable of provoking victims and destruction. They are placed across roadways and passages and can be active or passive, permanent or temporary and come under various technical and commercial names as bollards, wedge barriers, beam barriers, concrete Jersey barriers, ha-ha barriers etc. Moreover, they can even take the form of concrete sitting benches, flower planters, artistic elements, sculptures etc.

The material that is presented in the current document focuses on vehicle barriers that are mainly utilized for security and not safety purposes. The distinction between the two categories is a challenging task as they both share many common characteristics and they can satisfy different protection needs. Safety barriers are used for preventing and/or mitigating the results of an accident (errant vehicle) that can result in life loss, injuries or environmental destruction. On the other hand, vehicle security barriers are adopted for creating a physical obstacle against unauthorized entry and other form of relevant attacks, aiming at protecting human life and damage of property.

In light of the rising debate on effective solutions that could reduce and/or mitigate the risk from a vehicle-ramming attack and protection against vehicle borne improvised explosive devices (VBIED), the current guidance highlights the steps that should be followed towards the design and selection of appropriate tailor-made physical security barriers. In this chapter only the part concerning the site survey and the available protection measures is presented, as the risk assessment process has already been presented in Chapter 2.

## 4.2 Site survey

For selecting appropriate mitigation measures, several parameters need to be taken into account. The analysis of the urban layout surrounding a potential target leads to the realisation of critical locations and possible attack routes that might be used by the aggressors. Street geometry, urban density, natural obstacles (trees, vegetation) and land morphology are key elements affecting the attainable speed of a threat vehicle. Additional parameters that influence the approaching speed are vehicle acceleration, road surface slope and width, acceleration distance, turn radius etc. The combination of the calculated velocity and the mass of the vehicle provides its kinetic energy, which is essential for the selection of appropriate security barriers. An effective barrier should be able to absorb the kinetic energy of the speeding vehicle at the point of impact. If a certain penetration distance is allowed, the selected obstacle might be designed to cause significant damage to the threat vehicle so that it stops shortly after its impact. An alternative approach is to reduce the speed of a threat vehicle by appropriate measures before reaching the barrier, to avoid using massive solutions that are not visually appealing.

A close examination of the site layout that needs to be protected is a crucial step towards building a robust protection plan. A detailed map of the surrounding area is required for analysing the relative location of the various structural and non-structural elements that may affect the speed and direction of approaching vehicles, if a penetrative attack is of concern. The determination of threat vehicle lines, approaching angles, terrain type and road slope are important inputs when planning a site's security. The examined area should not be limited at the boundaries of the prospected security perimeter, but should be enlarged to include topographical features and potential routes of the threat vehicle. For attaining the required protection level, a holistic, creative approach is needed, that favours the assessment of possible attack scenarios and their consequences if successfully executed. The site layout investigation can be performed with various methods including, but not limited to, 2D and 3D assessments that may be performed either manually or by the assistance of computer software. The goal is to identify potential approach routes and their characteristics (terrain type, gradients, street obstacles, kerbs etc.) towards the asset to be protected or its hardened perimeter. CAD drawings or satellite images, like those included in Fig. 32, can provide the necessary information for accurately calculating the maximum vehicle speed and attack route at the asset location.

**Figure 32.** 2D and 3D satellite image of an area containing a potential target [OpenStreetMaps, Google Earth].



A site map can expose security vulnerabilities that potential terrorists may exploit as opportunities to strike, but needs to be regularly reviewed to guarantee that there are no significant changes in the vicinity of the potential target that might influence the effectiveness of the employed measures. For instance, the creation of a new square or the renovation of the area around the asset to be protected could result in new viable approach routes by a threat vehicle and approaching speeds that may exceed the capacity of the existing barriers.

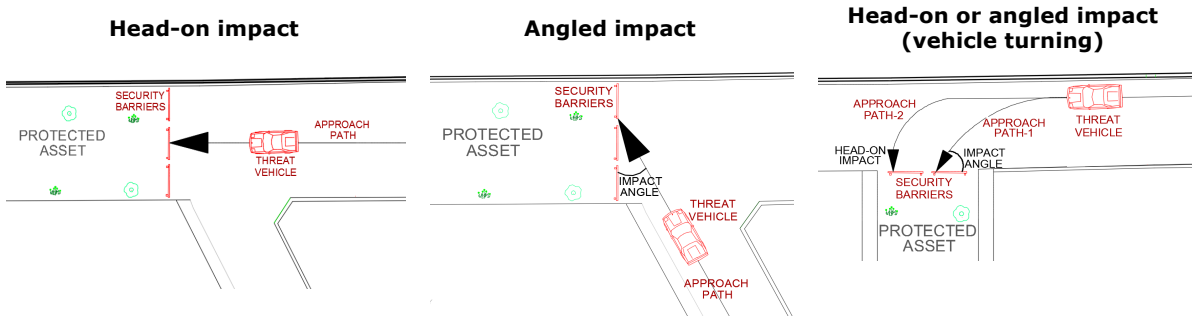
## 4.3 Attack scenarios

As has already been emphasized, identifying a terrorist threat and assessing the relevant risk poses great difficulties, since the time and place of an attack cannot be predicted with accuracy, especially since the aggressor's preferred tactic may change depending on many different factors. The use of vehicles for

performing an attack constitutes an attractive tactic, as they are easily acquirable and can penetrate unsecured public spaces causing great damage and high number of victims. For example, large trucks and buses that circulate city centres may be stolen and used for an attack, as their size guarantees the creation of extensive damage and large casualties in case of a ramming attack, while they can easily transport large explosive devices. Detection of threat vehicles is a challenging task, as such attacks are of opportunistic character and no extensive logistics or training of the aggressor is required.

Defining plausible vehicle attack scenarios includes evaluating the potential vehicle size, its maximum attainable speed and its angle of impact. In Fig. 33 the different impact modes and the angle of impact (which ranges between 0-90°) are schematically presented. The most severe is usually the head-on impact, which in the majority of cases is when the attack route is perpendicular to the target. If the angle of impact is different from 90° (angled impact), the energy that has to be absorbed by the selected security barrier may be lower (depending on the barrier's type). If the accelerating vehicle has to perform a manoeuvre before coming to contact with the protective barrier, it has to decelerate to avoid skidding or overturning (due to its lateral acceleration). In the third example shown in Fig. 33 the vehicle is travelling parallel to the installed barrier, which means that a quick turn is required when attempting to access the protected area of the asset. The radius of this turn is limited by the offset distance, i.e. the available road width that can be exploited by the aggressor before turning. As expected, the smaller the offset distance (because of the presence of inaccessible sidewalks or other obstacles), the smaller the radius of curvature and the smaller the vehicle attainable velocity (depending on the friction coefficient) in an effort to avoid skidding.

**Figure 33.** Vehicle modes of impact.

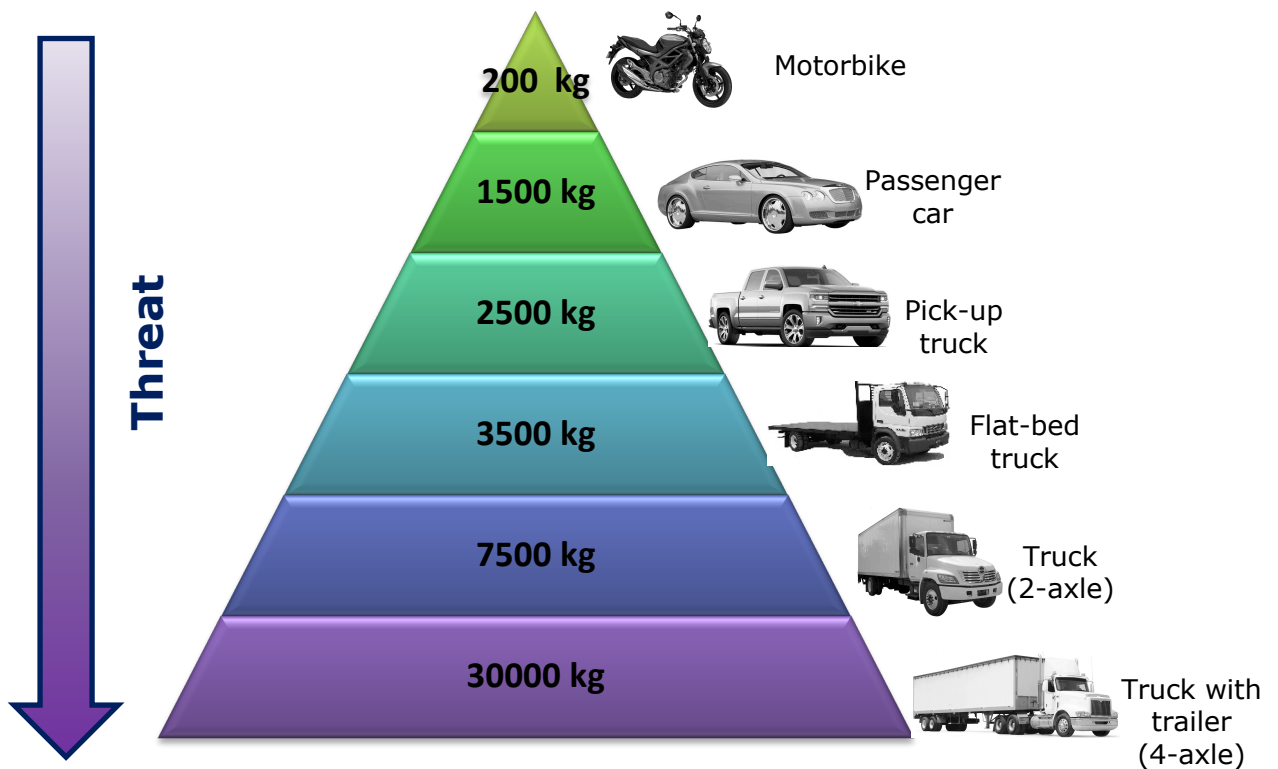


**4.3.1 Vehicle size**

A prerequisite during the selection of appropriate security barriers is the calculation of the vehicle's kinetic energy at the time of impact, which is associated with its velocity and its weight. This means that the kinetic energy of a large truck moving at a low speed may be equal to the energy of a smaller vehicle moving at a greater speed. For stopping the vehicle from approaching a protected target, the security barrier needs to be capable of absorbing its kinetic energy. In case of barriers that are not anchored to the ground, the greatest part of the kinetic energy is absorbed through the developed friction forces during the barrier's motion and may last several seconds. Alternatively, the speed of the attack vehicle may be reduced (through appropriate obstacles), so as to lower the security barrier performance requirements.

The calculation of the kinetic energy during impact entails the knowledge of the mass (or weight) of the threat vehicle. The vehicle types that could be used for performing an attack span from small passenger cars to heavy duty trucks carrying loaded trailers. Fig. 34 presents the weight of common vehicles, partly based on the recommendations of (CWA 16221, 2010). The presented values refer to the laden vehicle weights, which are required for assessing the kinetic energy in case of a penetrative attack. For evaluating the weight of a VBIED, one needs to resort to Fig. 10, where the upper limit weight of a potential VBIED carried by different means of transportation is presented.

**Figure 34.** Laden weight per vehicle type.



#### 4.3.2 Vehicle speed

The calculation of the speed of an approaching vehicle at the location of the barrier requires the estimation of a number of parameters, such as the initial velocity ( $v_0$ ), the average acceleration ( $a$ ) and the distance ( $s$ ) between the starting point of the vehicle and the barrier. Clearly, the final speed of the vehicle does not depend only on its size and its engine power, but also on the surrounding topography, such as the terrain type (asphalt, gravel etc.) and its conditions (straight, curved, wet, dry, sloped etc.). Since it is impractical to take into consideration all the parameters influencing a vehicle's attained speed, several conservative assumptions are usually made, that have to be revised in case of a detailed evaluation. By estimating the weight and the maximum attainable velocity of a threat vehicle, its kinetic energy can be calculated through the following equation,

$$KE = 0.039MV^2 \quad (6)$$

where,  $KE$  = vehicle kinetic energy [J]

$V$  = vehicle velocity [km/h]

$M$  = vehicle weight [kg]

Clearly, this is the well-known equation  $KE = \frac{1}{2}mv^2$ , expressed in different units ( $m$  = vehicle mass).

The speed at impact of a moving vehicle depends on its initial velocity, the travelled distance and its acceleration. However, the acceleration characteristics of a vehicle change depending on its type, its horsepower to weight ratio, its gear transmission type and its laden weight and usually do not remain constant through its entire motion. The acceleration profile of a moving vehicle is not constant, as at lower speeds the acceleration is higher and decreases with increasing speed. Medium to maximum acceleration rates are recorded when a

vehicle starts from rest and reduce as the speed increases. Moreover, if the path leading to the impact location is sloped, the velocity of a moving vehicle is affected due to the gravitational force and if the path is curved, the vehicle might experience skidding or overturning. More information on the methodology for calculating the speed at impact of an accelerating vehicle at different surface conditions and various readily available diagrams is available at (Karlos et al. 2018).

#### 4.4 Vehicle barrier types

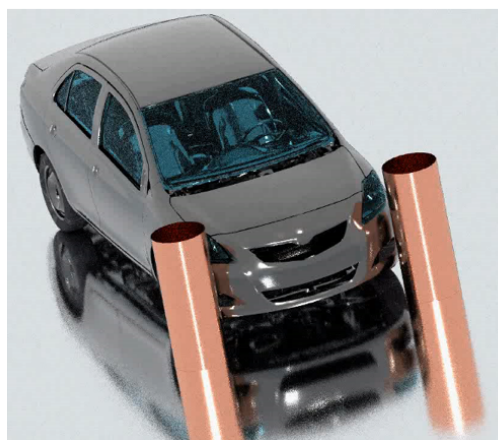
Vehicle barriers are devices or other structural obstacles that block or allow the controlled access of vehicles to an area that is designated as protected. These barriers need to be specifically designed and capable of stopping an ill-intentioned vehicle that attempts to breach the protected perimeter. Additionally, they can act as a deterrence, functioning as a psychological obstacle against aggressors who are planning an attack. Perimeter security focuses on introducing strategically placed obstacles that, ideally, are in harmony with the characteristics and architectural design of the surrounding landscape and provide protection against unauthorised vehicle (or even pedestrian) entrance. The main objective of the security barriers is absorbing the threat vehicle's kinetic energy and halting its penetration to the protected zone.

The installation of barriers requires specialized knowledge and can be a costly process, depending on the desired protection level. As the majority of available barrier solutions are not easy to be removed or modified, special attention should be paid during their selection and design process, while effort should be put into addressing the current and future threats.

Protective barriers may be physical (trees, rivers etc.) or manmade (bollards, planters etc) and they differentiate in shape, size, material and scope. They can be made of concrete, steel, rock, wood or any other stiff material that can effectively sustain the impact of a moving vehicle. In the case of physical barriers, the surrounding natural elements can also be used, such as vegetation, water, terrain, gravel. Vehicle barrier solutions can be divided into two broad categories regarding their operation: passive (static) and active (moveable).

The separation distance among the selected protective barriers is a crucial parameter, as it guarantees that no vehicle is capable of breaching the security perimeter without being damaged from impacting the security measures. This means that despite the fact that the largest and heaviest potential threat vehicle is usually selected for evaluating the maximum kinetic energy to be sustained by the barriers, it is the smallest vehicle (with the minimal width) that defines the maximum distance among neighboring barriers. Cars measuring less than 1.50m wide do not exist in the market (even though some specialized vehicles do exist), so the maximum separation distance among barriers (e.g. bollards) should be limited to a maximum distance of 1.40m, as verified by numerical simulations shown in Fig. 35. Moreover, if the barriers are placed on the sidewalk next to a street, a distance of 0.45m between the barrier and the edge of the sidewalk needs to be respected to allow for the safe passage of bicycles and motorbikes.

**Figure 35.** Vehicle modes of impact.



#### 4.4.1 Passive barriers

These barriers are not equipped with moving parts and can absorb the impacting energy either through proper foundation or by the combination of their weight and the road friction coefficient.

- **Bollards:** They constitute one of the most commonly used solutions for limiting the access of unauthorised vehicles in pedestrian areas, city centres, street pavements and reinforcing building perimeters. Their extensive use is attributed to their versatility, their effectiveness, their relatively easy manufacturing and installation and the wide selection of different shapes and decorations. They are usually fabricated from steel, reinforced concrete or a combination of the two materials (concrete core surrounded by a steel casing). Their narrow form and small size makes them less intrusive in comparison with other solutions, as long as their use is not exaggerated resulting in repetitive bollard rows that can be monotonous and unattractive. Their performance also depends on their foundation depth and size. Large foundations may be in conflict with underground utilities, so modern innovative solutions equipped with shallow bases are available, requiring smaller penetration depths.

**Figure 36.** Typical protective bollards.



- **Temporary barriers:** These barriers are re-deployable solutions that by nature lack foundation, so they rely on their mass in order to stop moving vehicles. These barrier types are frequently used in city centres, pedestrian precincts and during public events, as their temporary nature makes them impractical for the protection of building structures. If they are not anchored to the ground or connected to each other, their restraint capabilities are limited and can only stop light vehicles moving at relatively low speeds. Their objective is to gradually stop and damage a moving vehicle through the developed friction forces, which translates to relatively large penetration distances. However, their presence may act as a deterrence and can psychologically influence potential aggressors, but they also create a false sense of security to building inhabitants. The absence of footing, means that they can be used successfully for limiting the speed of approaching vehicles through appropriate placement, causing motorists to slow down before reaching the critical zone that has to be protected. The most frequent type of temporary barrier solutions are the Jersey barriers (developed originally for highway safety applications) that are precast concrete elements, commonly used during high profile social events or heightened security threats. Another type of temporary barriers that are popular in city-centres due to their attractiveness and easy manufacturing are planters that can be easily transported to the place of interest before being filled with soil. Over the last years, many different temporary barrier solutions have been used for access control purposes, such as plastic (water-filled) barriers, traffic spikes, fences, heavy trucks etc. The employment of a certain temporary barrier depends on the site protection needs, as established from the responsible security officials.

**Figure 37.** Typical temporary protective barriers.



- **Street furniture:** Hardened streetscape elements have the advantage to be smoothly integrated into urban design by being strategically placed in locations to intercept vehicle penetrative attacks. They comprise of dual-use elements, such as street lamp posts, bus stops, kiosks, signposts, walls, sculptures, trash bins, benches, flag poles, street art features, walls that ensure enhanced protection while having minimal visual impact. Special attention should be paid to the design of such elements, as they have to meet specific performance criteria so that they are not over-scaled and/or over-designed. They can also be used as supplementary components to other solutions, such as bollards, to improve the attractiveness of the security measures.

**Figure 38.** Typical street furniture elements.



- **Landscape and trees:** The use of topography for upgrading the security of a certain site is one of the most unobtrusive solutions, as the additional protective elements can be harmonically integrated into the surrounding urban environment. If natural formations that can be used as barriers (e.g. rivers, lakes, forests) are absent, terrain can be appropriately shaped to create ditches and sloped formations (berms) that will be impossible to be traversed by a moving vehicle. The ditch needs to be wide enough (dimensions depend on the vehicle's type and speed) so that an approaching vehicle cannot cross it. The construction of a berm aims at capturing the front, rear or underside of the vehicle's chassis when attempting to overcome it, so its design has to respect certain aspects, such as its approach angle ( $\geq 50^\circ$ ) and height ( $\geq 1.25\text{m}$ ). Protection can also be provided by appropriately changing the topographical features of a site, such as creating elevated areas, shaping grass lawns, planting trees. Vegetation can also be an efficient and cost-effective solution, but requires maintenance and should be properly designed to avoid the formulation of dark areas of concealment where the sight of security guards is blocked. Nevertheless, the use of individual trees as a barrier is questionable, as their performance has many uncertainties and it depends on their health, the soil conditions, their roots etc., so only the adoption of densely planted trees is recommended. Water features (pools, fountains, ponds, streams, channels etc.) can also be employed as countermeasures against incidents of unauthorised vehicle and people entry, but need to be properly maintained. A major drawback to the use of landscape for enhancing the security characteristics of a site are the increased space requirements. That practically means that in city centres, where the available space is limited, such measures require an overall revision of the urban management plan, which is not always feasible.

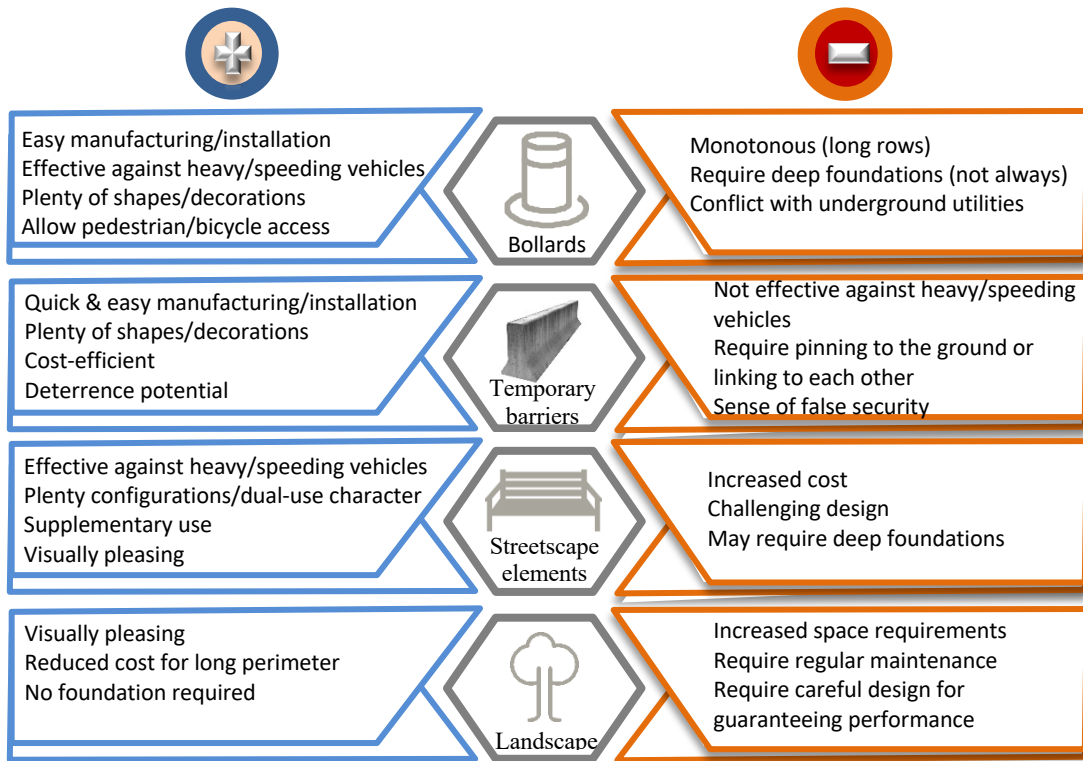


**Figure 39.** Typical landscape protective solutions.



European cities and private companies are commonly investing in passive barriers in order to enhance the security of public spaces or enforcing a stand-off distance from a sensitive asset. The versatility of the described solutions is partly responsible for their popularity and application in different environments. Fig. 40 summarizes some of the most prominent advantages and limitations of the most frequently used passive barriers.

**Figure 40.** Advantages and disadvantages of passive barrier solutions.



#### 4.4.2 Active barriers

Active barriers are equipped with moving parts, as they are usually adopted in areas where access of authorised vehicles is desired, or access is only granted for certain time periods. They might be controlled by the driver of the authorised vehicle (i.e. entrance to a garage or of buses in pedestrian areas), by an automatic electronic system or by security guards that are responsible for inspecting incoming traffic (i.e. control points before entering a site). Due to the moving parts, considerable maintenance of the mechanical system is required to guarantee its reliable performance.

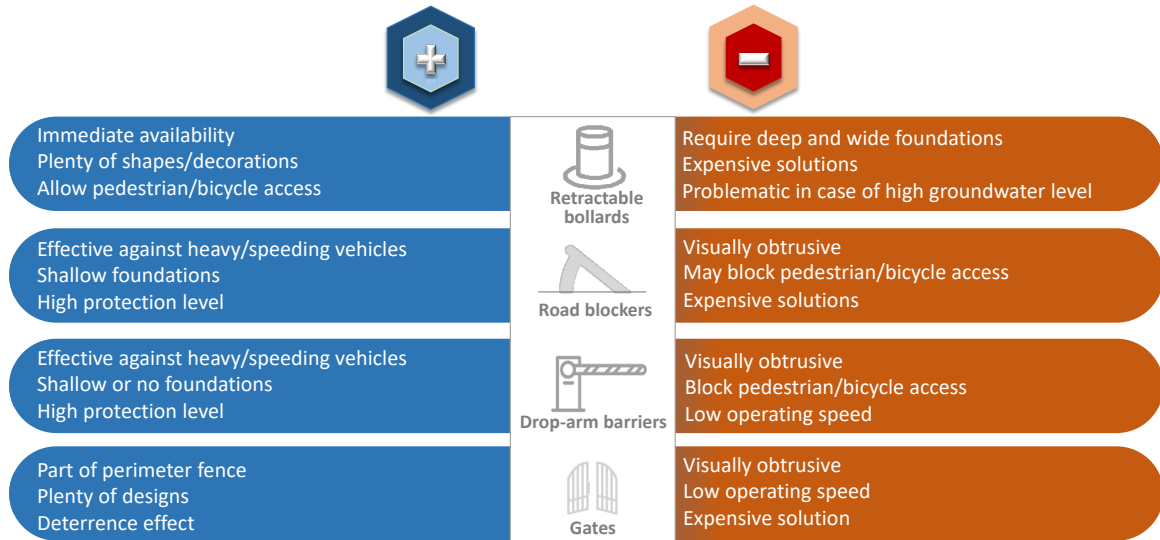
- **Retractable bollards:** During their operation, these bollard types should remain in a raised position and be lowered to allow vehicle entrance after completion of the screening process. They can be either manually lowered, which is common in case of infrequent traffic, or by using a hydraulic or pneumatic unit, such as in site entrances with heavy traffic requirements. One of their greatest advantages is the fact that they permit pedestrian entry irrespective of their position (raised or retracted), but are usually an expensive option as they require deep and wide foundations.
- **Road blockers:** These high security ramp systems are characterized by a metal plate that is visible at the surface of the road. When raised, using hydraulic or electrical systems, this metal plate is angled upwards and disables unauthorised vehicle entrance. Permanently installed road blockers (also known as wedge barriers) can provide a high protection level, without requiring deep foundations, while portable, surface mounted systems are also available. Due to their size when deployed, they are visually obtrusive compared to other barriers and may block both pedestrian and bike access.
- **Drop arm barriers:** These barriers consist of a steel arm that is usually supported by properly anchored concrete elements. The steel beam is raised either manually or by the use of pneumatic or hydraulic mechanisms. Similar barriers are commonly used in parking lots, shopping malls and toll stations, but they lack the stopping power of the certified, reinforced, concrete-anchored versions.
- **Gates/fences:** Gates are a common security element providing perimeter protection, as they are adopted for limiting the entrance of approaching vehicles. They are usually part of a perimeter fence system and can be operated either manually or automatically. Attention is needed when selecting a gate capable of stopping incoming threat vehicles, as many of the commercially available systems provide low protection and are characterized by low operating speeds.

**Figure 41.** Typical active barriers.



Active barrier systems are commonly used in access control zones to exclude the entrance of threat vehicles that might carry an IED. The most commonly advantages and limitations of such systems are summarized in Fig. 42.

**Figure 42.** Advantages and disadvantages of active barrier solutions.



### 4.4.3 Innovative barriers

Apart from the above-mentioned traditional solutions, many modern innovative passive and active systems have been developed in the last years that are able to satisfy the emerging new threats in global terrorism. These barriers combine the advantages of some of the most commonly used solutions, providing increased efficiency, reduced cost and improved appearance. Many systems take advantage of dual-use technologies providing increased protection in a visually attractive manner. Special attention has been recently paid to the development of temporary solutions that can be used for effectively protecting people engaged in social events, as it has been demonstrated that terrorists target public spaces. Many of these solutions can be quickly deployed without the need for foundations or other form of buttresses, while they allow free access to people and bicycles. Other solutions focus on providing elevated protection while remaining hidden in specially designed artistic elements or aim at intercepting a speeding vehicle by puncturing its tyres and destroying its steering system. The effectiveness of these systems can be determined through their performance rating in standardized crash tests. In the following figure, three such systems are displayed; the first is a lightweight, surface-mounted barrier solution employed for providing temporary security during public events, the second is a deployable spike net that can thwart a vehicle attack and the third is a portable, movable barrier.

**Figure 43.** Examples of innovative protective barriers.



### 4.5 Barrier certification

There exist various test specifications (IWA 14-1, 2013), (PAS 68, 2013), (CWA 16221, 2010) and (ASTM F2656, 2018) that have been developed for quantifying and certifying the performance of vehicle barriers through impact tests. Since a universally accepted methodology is still missing, commercially available security barriers may have been tested under different scenarios (depending on the standard used), which means that they are accompanied by different abbreviations to display their performance. The proposed testing protocols included in each document are mainly destined to assess the single impact performance of permanent solutions

developed for building perimeter protection and not the performance of movable, temporary barriers. Table 13 includes the documents that are most commonly used for testing of vehicle barriers. These documents need to be revised on a regular basis in order to maintain their active status, which means that the renewal of non-revised documents is still pending, as seen in the following table.

**Table 13.** Specifications for vehicle security barrier impact assessment.

Abbreviation	Type of technical specification	Standardization body	Valid until
IWA 14-1:2013	Workshop agreement	ISO (International Organization for Standardization)	12/2019*
PAS 68:2013	Consultative document	BSI (British Standards Institute)	08/2016
CWA 16221	Workshop agreement	CEN (European Committee for Standardization)	08/2017
ASTM F2656	Standard	ASTM (American Society for Testing and Materials)	01/2023

\*(currently under revision)

The performance assessment of vehicle security barriers is demonstrated with the use of certain abbreviations, which are summarized in Table 14. (IWA 14-1, 2013), (PAS 68, 2013) and (CWA 16221, 2010) adopt nearly identical abbreviations for summarising the performance of tested barriers, whereas (ASTM2656, 2018) provides somewhat less information.

**Table 14.** Abbreviations for barrier performance ratings.

<p><b>IWA 14-1:2013</b></p> <p><b>PAS 68:2013</b></p> <p><b>CWA 16221</b></p>	<p><u>X/VSB/W[A]/V/θ:P/D</u></p> <p><u>X/VSB/[A]W/V/θ:P/D</u></p> <p>where: X = test type</p> <p>VSB = security barrier type</p> <p>A = vehicle classification</p> <p>W = vehicle weight [kg]</p> <p>V = vehicle velocity [km/h]</p> <p>θ = angle of impact [deg]</p> <p>P = vehicle penetration [m]</p> <p>D = dispersion of debris [m]</p>
<p><b>ASTM F2656</b></p>	<p><u>A/V/P</u></p> <p>where: A = vehicle classification</p> <p>V = vehicle velocity [mph]</p> <p>P = penetration rating</p>

The test type (X) refers to the method that was used for the experimental evaluation of a barrier's performance, for which the letter "V" is usually adopted, which stands for "vehicle impact test". The security barrier type (VSB) represents the barrier model that was tested, as described in Section 4.4 (fixed bollards, blockers etc.). The predefined tested vehicle's weight (W) and classification (A) are different among the examined standards as shown in Table 15. The actual weight of a test vehicle may vary slightly from the values of Table 14, because different tolerances are introduced among the various standards as shown in the parentheses. Vehicle speed (V) at the time of impact is included in the abbreviations proposed by all standards and their predefined values are presented in Table 15. Similar to the vehicle's weight, the allowable speed tolerances among the examined specifications are different.

**Table 15.** Vehicle classes and relevant weight.

Test standard	Vehicle type	Vehicle classification	Vehicle weight [kg]	Vehicle test speed [km/h]
<b>IWA 14-1:2013</b>	Car	M1	1500 (±75)	16,32,48,64,80,96,112
	Pick-up	N1G	2500 (±75)	16,32,48,64,80,96,112
	Flat bed	N1	3500 (±100)	16,32,48,64,80,96
	Day cab	N2A,N2B,N3C,N3D	7200 (±400)	16,32,48,64,80
	Day cab	N3E	24000 (±400)	16,32,48,64,80
	Day cab	N3F	30000 (±400)	16,32,48,64,80
<b>CWA 16221 PAS 68</b>	Car	M1	1500 (±50)	16,32,48,64,80,96,112
	Pick-up	N1G	2500 (±50)	16,32,48,64,80,96,112
	Flat bed	N1	3500 (±100)	16,32,48,64,80,96
	Day cab	N2	7500 (±100*)	16,32,48,64
	Day cab	N3 (2-axle)	7500 (±150)	16,32,48,64,80
	Day cab	N3 (4-axle)	30000 (±600)	16,32,48,64,80
<b>ASTM F2656</b>	Car	SC	1100 (±25)	50,65,80,100
	Sedan	FS	2100 (±50)	50,65,80,100
	Pick-up	PU	2270 (±50)	50,65,80,100
	Standard truck	M	6800 (±140)	50,65,80
	Class 7 cab-over	C7	7200 (±150)	50,65,80
	Heavy truck	H	29500 (±590)	50,65,80

\*At PAS 68 (±150)

Since the test vehicle's weight and speed are available from each test, its kinetic energy at impact can be calculated using Equation (6). The certification of a protective barrier demonstrates its performance when impacted by a vehicle of a certain weight and speed. Table 16 presents the kinetic energies associated to the vehicle classes and velocities proposed in the various testing standards, which may serve as an upper bound

during the selection process of protective barriers. These values may be compared with the kinetic energy calculated through the developed attack scenario to determine the most appropriate security barrier.

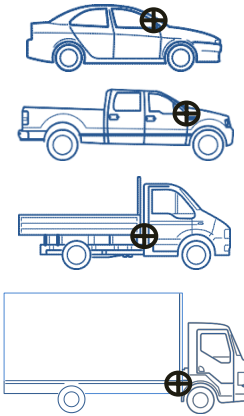
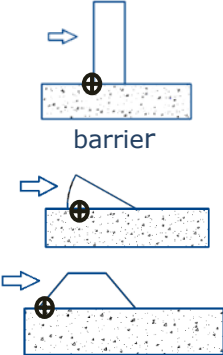
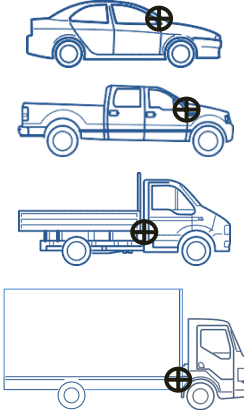
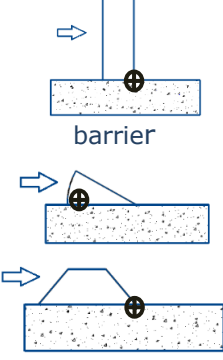
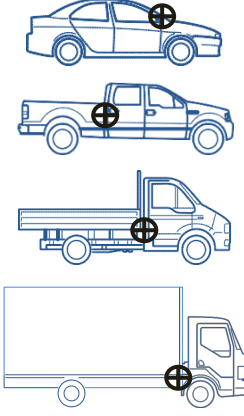
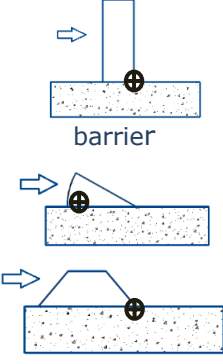
**Table 16.** Vehicle kinetic energy [kJ].

Test standard	Vehicle speed [km/h]	Vehicle classification					
		M1	N1G	N1	N2A,N2B, N3C,N3D	N3E	N3F
<b>IWA 14-1:2013</b>	<b>16</b>	15.0	25.0	34.9	71.9	239.6	299.5
	<b>32</b>	59.9	99.8	139.8	287.5	958.5	1198.1
	<b>48</b>	134.8	224.6	314.5	647.0	2156.5	2695.7
	<b>64</b>	239.6	399.4	559.1	1150.2	3833.8	4792.3
	<b>80</b>	374.4	624.0	873.6	1797.1	5990.4	7488.0
	<b>96</b>	539.1	898.6	1258.0	-	-	-
	<b>112</b>	733.8	1223.0	-	-	-	-
<b>CWA 16221 PAS 68</b>	<b>16</b>	15.0	25.0	34.9	74.9	74.9	299.5
	<b>32</b>	59.9	99.8	139.8	299.5	299.5	1198.1
	<b>48</b>	134.8	224.6	314.5	673.9	673.9	2695.7
	<b>64</b>	239.6	399.4	559.1	1198.1	1198.1	4792.3
	<b>80</b>	374.4	624.0	873.6	1872.0	1872.0	7488.0
	<b>96</b>	539.1	898.6	1258.0	-	-	-
	<b>112</b>	733.8	1223.0	-	-	-	-
<b>ASTM F2656</b>	<b>50</b>	107.2	204.7	224.2	663.0	702.0	2876.2
	<b>65</b>	181.2	346.0	379.0	1120.5	1186.4	4860.9
	<b>80</b>	274.6	524.2	544.1	1697.3	1797.1	7363.2
	<b>100</b>	429.0	819.0	897.0	-	-	-

Vehicle penetration (*P*) describes the distance travelled from the attack vehicle after its impact with the security barrier and until it stops. Depending on the applicable testing standard, this distance is measured from the front or the back face of the barrier up to a reference point on the vehicle, located either on the base of the A pillar

or the front edge of the load platform. It is interesting to note that the location of the reference points depends on the vehicle's category and is uniform among the different testing standards, with the exception of pick-up trucks. Moreover, (ASTM F2656, 2018) is the only standard that proposes a penetration rating system, depending on the distance covered from the vehicle after coming to contact to the security barrier. The dispersion of major debris (*D*) is proposed by three of the examined testing standards (IWA 14-1, PAS 68 and CWA 16221), as a parameter showing the distance of detached vehicle, ballast or barrier pieces of significant size (weight  $\geq 25\text{kg}$ ) from the barrier datum line. Table 17 shows the location of the reference points used for calculating the penetration distance among the different standards and the relevant penetration rating, where applicable.

**Table 17.** Reference point locations and penetration rating.

Test standard	Vehicle reference point	Barrier reference point	Penetration rating
<p style="text-align: center;"><b>IWA 14-1:2013</b></p>		<p>Front face of</p>  <p style="text-align: center;">barrier</p>	-
<p style="text-align: center;"><b>CWA 16221 PAS 68</b></p>		<p>Back face of</p>  <p style="text-align: center;">barrier</p>	-
<p style="text-align: center;"><b>ASTM F2656</b></p>		<p>Back face of</p>  <p style="text-align: center;">barrier</p>	<p><b>P1</b> (<math>P \leq 1\text{m}</math>)  <b>P2</b> (<math>0\text{m} &lt; P \leq 7\text{m}</math>)  <b>P3</b> (<math>7\text{m} &lt; P \leq 30\text{m}</math>)</p>

Still, the resulting penetration distance and response of each security barrier does not depend only on the weight, class and velocity of the test vehicles in the various standards as by focusing solely on those characteristics we fail to take into account other important components that might significantly affect the vehicle-barrier interaction, such as the geometrical features of the test vehicles. Cars, vans, pick-ups and trucks used in crash tests performed in America are usually characterized by larger dimensions, higher mass centres, different motor geometries etc., with respect to vehicles used in European testing centres, which means that considerable variations in barrier performance should not be excluded. To avoid such discrepancies, it is recommended that the barrier selection corresponds to the predominant vehicle types in the country of interest. As a result, countries where US-type vehicles are the majority, barriers tested according to the ASTM standard should be favoured, whereas in countries that most of the circulating vehicles are European/Asian-type, barriers certified according to the PAS, CWA or IWA standards constitute a more suitable option.

#### **Examples:**

- A security barrier is tested according to (IWA 14-1, 2013) and its performance rating is indicated as: "bollard V/3500/N1/64/90:4.5/2.2"  
This means that the barrier type [bollard] was tested under vehicle impact test [V] with a flat-bed vehicle [N1] weighing 3500kg with a speed at the time of impact equal to 64km/h. The impact angle was equal to 90° and the distance travelled by the vehicle from the time of impact until coming to a halt (distance between the front face of the barrier and the front edge of the load bed) is equal to 4.5m. Major debris (>25kg) were also detached and landed 2.2m from the front face of the barrier.
- A security barrier is tested according to ASTM F2656 and its performance rating is indicated as: "M/40/P2"  
This means that the barrier was tested under vehicle impact test with a medium-duty truck [M] weighing 6800kg moving at 65km/h (equal to 40mph) at the time of impact. The penetration rating of the barrier (P2) indicates that the distance between the leading lower bed edge of the vehicle and the back face of the barrier is  $1.0m < P \leq 7.0m$ . Even though the impact angle is not explicitly displayed in the performance rating, unless otherwise mentioned, its value is equal to 90° (perpendicular impact).

Up to now the performance of barriers against potential threat vehicles is officially assessed through physical impact tests as outlined in detail in the abovementioned documents. Crash-testing guarantees that the barriers are tested under real life conditions and that all complex phenomena related to the behaviour of both the vehicle and the barrier are taken into account. However, such experiments are very expensive and consequently, only a limited number of attack scenarios and protective measure geometries are usually evaluated.

Over the last few years, computational methods have been successfully employed for assessing and verifying the performance of structural and non-structural components during various dynamic and nonlinear events, such as blasts, airplane collisions and crash simulations. The automotive industry has been extensively using state-of-the-art computer simulations in order to improve the crashworthiness of its vehicles under different crash scenarios, while minimizing the costs stemming from actual crash tests. Similarly, the capabilities of numerical models may be also exploited in the case of vehicle/barrier interaction, after verifying their validity through comparison with actual crash test data. Reaching a high level of confidence in the numerical solutions requires the use of reliable and effective finite element algorithms that need to be examined in contrast with physical experiments. Such techniques should be promoted during the barrier design process as they may considerably reduce the number of tests and contribute to the manufacturing of effective and cost-efficient protective solutions. A numerical framework for studying the impact performance of vehicles, including the desired parameters of the numerical model and the computational efficiency of the analysis can be found in (Valsamos et al., 2020).



## **5 Protection against unauthorised entry and ballistic attacks**

### **5.1 General**

In modern society, protecting a facility from the unauthorised entry of persons with malicious intent can be accomplished by a combination of physical security systems and digital technologies. New digital capabilities provide innovative tools to efficiently respond to the challenges that arise when trying to setup and maintain a security perimeter around a valuable asset. Integrating video surveillance and other digital security systems in a multi-layered approach for securing a building's perimeter may result in a substantial increase in the efficiency of deterring, detecting and responding to threats. Several technologies are available nowadays that can have a supplementary role to the physical security measures, many of which have been presented in previous chapters. These technologies include, but are not limited to, video surveillance, intrusion detection, access control, sound detection, CBRN (chemical, biological, radiological and nuclear) sensors and video analytics.

Digital technologies provide the opportunity to retrieve immense amount of data in real time which, if analysed properly, can produce sense-making information facilitating informed and timely decisions. The derived data may significantly improve threat detection and communication, enhancing the coordination and collaboration among various authorities. A crucial role in taking full advantage of the potential of each digital security system plays the installed software and its efficiency. Accurate detection, precise information, real-time reaction, minimal glitches and false alarm rate depend on the software technology and its adaptability to the existing environment. The simultaneous use of various security systems and their harmonic cooperation requires an effective and immediate sharing of data, which can be extremely complex due to compatibility issues. Successful management of the different employed systems may be accomplished by using robust data processing platforms and skilled professionals that are able to handle the flux of incoming information, which in some cases may also be contradicting. Security systems are only a small integrated part of a well-planned security scheme and are an invaluable tool in supporting decision makers in emergency cases.

### **5.2 Physical protection measures**

Addressing a site's vulnerabilities through the introduction of physical protective measures is a key tool for reducing the risk of unauthorised people access and ballistic threats. Perimeter security can be realized through different design strategies, that span from the installation of specialized barriers to the redesign of the surrounding landscape in a security-by-design concept. The previous chapter provided an extensive summary of solutions that are used for blocking vehicular access and may also be employed for denying the access to potential pedestrian intruders. Clearly, some of the proposed solutions (e.g. bollards, road blockers) are not effective against hostile pedestrian attacks, while others (e.g. fences and gates) can deter and delay intruders from gaining access to the facility. This aspect demonstrates that the selection and the design of the barrier system needs to correspond to the assessed threat. Moreover, the selected protection measures need to be in line with the architectural and landscaping features of the asset's surrounding environment, as they are its first visible aspects and define its identity.

A typical physical perimeter protection system for denying pedestrian access consists of two main elements; the surrounding fence and the control gates, where people (and usually vehicles) are screened before entering the site. Properly designed fences and dense vegetation can deter and delay intrusion, while they could be equipped with concealed sensors and warning systems to further enhance the protection level, as will be described in the next sections. Certified anti-ram fences are only required if hostile vehicle threats are also deemed as probable, since the cost of crash-rated systems is much higher.

The building's exterior may also be secured to protect against unauthorised entrance in case of absence of a surrounding fence or if such fence is breached. This means that secure locks need to be installed in the doors that lead outside the building, though should easily open in case of an emergency evacuation. Moreover, barriers may be applied to man-sized openings, while doors and facades resistant to manual attacks and bullet resistant glazing may be introduced, as shown in Tables 7 and 8. Section 3.8.2 provided additional advice on the design of access control zones against blast loads. Additional films may also be applied to external windows and doors to provide protection against eavesdropping as certain devices can capture conversations from a great distance. Restricting the entry through external doors and windows channels the access to specialized areas, where screening procedures are enforced. These areas need to be designed to address ballistic threats through the introduction of bullet proof glazing and contain intruders by blocking their access to the core of the building.


Access control points provide controlled entry to the building premises and are usually equipped with CCTV, metal detectors, communication facilities etc. and should be designed so as not to create delays during the inspection process. Delaying building penetration from intruders provides occupants more time to seek cover and escape, while grants law enforcement and response units time to react more effectively. As a result, the design of safe heavens and escape routes within the building's interior are strategies that need to be adopted, both for security and safety purposes.

### **5.3 Video surveillance**

In the last years, video security technology has been revolutionized with the introduction of high computing power, huge memory potential and ample processing capabilities. The need for elevated security at a reduced cost has led to the installation of closed-circuit television (CCTV) systems at many private and public spaces. Their popularity is a result of their remarkable ability to constantly monitor in real-time large areas with a minimum number of personnel, which translates to a significant decrease in inspection expenses. A video surveillance system usually consists of the camera, the transmission media, the image analysis equipment, the monitor and a recorder.

Cameras are the most exposed elements of a video surveillance system and need to be carefully selected keeping in mind the geometry of the area where they will be installed. The wide variety of available cameras and their different functionalities makes selection challenging, as they have to fulfil the expectations of the user (depending on the considered threat), which in many cases are not accurately defined. One of the first considerations is the level of detail, the installation point, the desired view and consequently whether it needs to be fixed, equipped with rotating/zooming capacity or multi-lens technology. The quality of the video image does not only depend on the resolution (HD, Full HD, 4K etc.) of the camera, but also on the surrounding lighting, the contrast of the various items relative to the background, the complexity of the environment and the movement of the objects or personnel. This means that selecting the camera's resolution depends on the intended application (detection, face or number plate recognition etc.), as a detailed monitoring requires better image quality. It is highlighted that stored images can only be zoomed digitally (in contrast with real-time recordings), so their resolution needs to be high enough to provide crisp and clear results. The operational conditions also designate the imaging and light sensitivity requirements, as there are visual monochrome and colour cameras, models that can function under night-time conditions with extremely low light demands (ICCD cameras), and cameras that use thermal sensors and can operate in total darkness (thermal cameras). The transmission of the video signal (analog or digital) to the monitor may have to be broadcasted through buildings, the ground etc., so the hardware to be used (cables, fiber optic, LAN, internet, wireless etc.) needs to be carefully selected to satisfy the video signal quality requirements. Table 18 demonstrates the most important characteristics of the surveyed area and the viewing equipment that have to be considered from the decision makers before setting up a video surveillance system.

**Table 18.** Video surveillance considerations.



Considerations	Available features
Intended use	Detection, face recognition, plate recognition
Area characteristics	Lighting, reflections, objects in motion, temperature, area size, weather conditions
Illumination	Natural light, artificial light, total darkness
Field of view	Fixed, 360° rotation (pan-tilt-zoom), panoramic lens
Image quality-resolution	LCD, HD, Full HD, 4K etc.
Light demands	Monochrome, colour, night-time, thermal
Video signal	Analog, digital
Transmission	Cable, fiber optic, LAN, wireless, internet
Monitors	Size, resolution (Full HD, 4K etc.)
Recorders	Hard drive, optical disk, cloud
Other considerations	Camera housing, power supply, vandalism

The video surveillance system is often connected with a video analysis software that is able to process the information and carry out specific security controls. Technological developments in the field of software applications allow the system to react in real-time and notify the security operator concerning its findings. Such systems are widely used to automatically recognize number plates of vehicles that enter into restricted access zones (e.g. in historic city centres), for speed checks and police enforcement purposes. The algorithms that are used for the security checks can be divided in three distinct categories, as shown in Table 19 and manage to perform specific assignments. Their wide potential and functionalities is demonstrated by their extensive use in different fields, spanning from home automation systems to transport and security.

**Table 19.** Video analysis algorithm types.

Specific algorithms	Have a specific assignment/Check for specific behaviour (e.g. motion detection, intrusion/line crossing, unattended objects, object/person tracking, object acquisition, people congregation, number plate recognition, loitering, illegal parking)
Artificial intelligence	Algorithms that learn to detect abnormal behaviour and alert the security officer. They require an initial 'learning' period in order to distinguish common from uncommon situations.
Facial recognition	Systems that use algorithms to compare facial characteristics with stored images in their database. Modern systems are able to do that in real-time and even under low light conditions or individuals in motion.

Video surveillance systems may encounter technical problems regarding the lack of accuracy or blind spots in the recording. The integration of different systems may also cause discrepancies in the used format and difficulties in the analysis. The use of multiple cameras usually results in lack of data storage, especially if the videos are of high resolution. Stored videos are generally deleted after some days to make space for new ones, which makes the analysis of past incidents troublesome. New artificial intelligence (AI)-based analytics software however, can help in reducing the need for constantly monitoring and storing video footage and reduce the need for ample data storage.

The installation of a video surveillance system needs to respect the current legislation and target clearly defined areas that are considered to be of security importance, so as to minimize recording of unnecessary footage. A notice should be clearly displayed to inform the individuals entering a private or public area that video surveillance is being used. The aim of CCTV systems is to enhance the security in a certain area and not intrude in people's private life and violate their fundamental rights. More information concerning the processing of personal data through video devices can be found in the relevant guidelines that have been published by the European Data Protection Board (EDPB, 2019).

#### **5.4 Access control and intrusion detection systems**

Access control systems are employed at the perimeter of an asset in order to guarantee the accessibility to accredited personnel and minimize the possibility of a physical intrusion. They may be controlled locally by a security officer/guard, from a central control room or through a fully automatic installation. Access control systems do not only prevent unauthorised people entry, but also of IEDs or other harmful material and devices carried by potential aggressors. In case of relevant threats, the incoming packages and personal belongings may be controlled at the entrance of the facility (e.g. through X-ray machines), vehicles may be inspected and their parking may be limited. The level of security depends on the potential threats, the importance of the asset and the parameters that were presented during the risk assessment process in Chapter 2.

Intrusion detection and access control are complementary systems that serve in alerting the security officials for any breach in the enforced perimeter and providing access to identified personnel respectively. The most common method of granting access to a facility is through a card or badge that may be visually controlled by a security guard or a card reader. These card readers may be operated through a magnetic stripe/proximity reader, a touchpad to insert codes or even a biometric scanner (fingerprint or retina). A proper procedure has to be designed to grant access to people that do not enter the asset on a daily basis, such as visitors, VIPs and contractors. To ensure that access to restricted areas is prohibited, various intrusion detection systems may be used together with the protective measures described in section 5.2, such as laser scanners, motion and radar detectors, magnetic contacts, pressure-sensitive mats, trip wire sensors, volumetric surveillance and glass break sensors. Clearly, the type and access control requirements are defined by the relevant threat, the vulnerabilities and significance of the protected facility or area.

Another common method for screening persons before entering a site is the use of security scanners, similar to those adopted in airports. These scanners are authorised under certain operational conditions and detection performance standards that are designed for being used mainly in airports. For instance, security scanners shall not store, retain, copy, print or retrieve images and any unauthorised access and use of these images is strictly prohibited. Screening can be performed through full-body scanners (millimetre-wave or X-ray) that can detect both metallic and non-metallic objects concealed on a person’s body or via walk-through and hand-held metal detectors. Similarly, X-ray machines and explosive detectors may be used for the screening of luggage, the former providing operators the option to visually examine the contents of luggage through an imaging software and the latter as a supplementary tool to improve the effectiveness of the inspection. The operational effectiveness and the detection performance capability depend both on the employed technology and the qualification and training of the security staff handling the equipment. To ensure reliable security performance and protection of citizen rights, detailed regulations exist in the European Union regarding the use of security scanners in European airports, that can provide useful information during the selection and installation of security scanners in the access control zones of private sites.

Access control may also be applied in the area surrounding the restricted core of the facility. This includes managing vehicle access, through a control system that needs to be selected based on a detailed traffic management plan, taking into consideration the type of drivers, vehicles and their frequency of passing through the control points. It also includes employing some of the hostile vehicle mitigation options that were described in Chapter 4 (e.g. fences, bollards, gates). The type of access control at the entrances of a site can significantly affect the traffic throughput and cause delays, especially during peak flow times or special occasions (e.g. VIPs, visitors, external personnel, misplaced badges and emergency services). Table 20 shows the effect of access control types on the vehicle transit time that may cause queues, bottlenecks and additional security vulnerabilities, as stated in (IWA 14-2, 2013).

**Table 20.** Effect of access control types on vehicle transit time.

	<b>Estimated vehicle transit time (sec, ±25%)</b>	<b>Vehicle per minute (±25%)</b>
<b>Nothing</b>	1	60
<b>Visual pass check</b>	4	15
<b>Hands-on/card reader pass check</b>	8	7
<b>Check and single line security barrier</b>	19	3

As security demands in modern societies are becoming higher, they will inevitably lead to the use of multiple layers of security systems. Their advanced technological aspects and state-of-the-art software poses great difficulties in their efficient cooperation and networking. The aim is to develop a single control system that will incorporate different security features (video surveillance, access control, intrusion detection etc.), but will be easily managed by a single individual having all the information readily available in real-time.

**5.5 CBRN-E sensors**

In the last years there have been developed several technologies for detecting and consecutively preventing and responding to CBRN-E threats. These threats include more than one thousand agents that need to be traced by specialized equipment. In the past, these detection technologies were handled exclusively by the secret services and specially trained security officials. Due to the technological advancements in the field of detectors, the analysis of substances takes place almost real-time without the need of lengthy, sophisticated procedures that were required in the past. To facilitate better understanding and improved cooperation between Member

States the European Commission issued a dedicated Action Plan that proposes several actions to contribute to the preparedness and resilience in case of an attack (European Commission, COM 610, 2017).

There exist various technologies that can be employed for detecting the presence of dangerous agents, such as the use of Ion spectrometry for tracing chemicals and explosives, gamma-ray spectrometry for radiological agents or polymerase chain reaction assays for detecting biological threats. According to a study from the Defence Advanced Research Projects Agency (DARPA, 2010), there is a number of key metrics that define the efficiency of a detector (sensitivity, probability of detection, false positive rate and response time) and several other characteristics that define its operation (purchase and operation cost, maintenance requirements, reliability, size, weight and power consumption). A list of the different available standards that have been developed in the last years for CBRN-E detectors can be found in (Coursey et al. 2016).

Such technologies are extensively used in the civil aviation field to identify the unique attributes and chemical components of CBRN-E agents (focusing mainly on detection of explosives and weapons). There are plenty of equipment available in the market that can successfully detect the majority of hazardous agents. Selecting an appropriate sensor depends on the established attack scenario and the relevant risk analysis. Attacks with the use of CBRN-E agents are of low probability but could potentially have a great societal impact. The detection of an ample range of agents may require the use of multiple systems that have to work together through a dedicated interface, which may increase operational complexity. The optimal and accurate sensor placement following a detailed study on the facility's needs, is essential for minimizing their number (combination of protected area and sensor coverage range) and keeping low the initial, operational and maintenance cost.

## **5.6 Audio monitoring**

A new trend has recently appeared in using audio equipment for enhancing the security characteristics of a site. Audio monitoring, when combined with appropriate software, can automatically filter natural/common noises and distinguish abnormal sounds that are of human (e.g. a scream) or other (e.g. class breaking, gunshots, explosions) origin. Sounds are screened and classified based on their acoustic features, several of which are available in the open literature, and trigger an alarm if they correspond to certain characteristics.

The advantage of audio surveillance systems is that they can still operate under low or no light conditions, where video systems may not provide clear images, and they can have a supporting role to images captured by CCTV, providing additional verification in case of an incident. The effectiveness of such systems is lower in noisy environments with multiple sound sources, as they have to separate background noise from the alarm-triggering sounds. However, recent technological advancements and machine learning techniques have allowed the development of specialized algorithms that can accurately identify the sounds of interest and minimize errors. As already underlined during describing video surveillance systems, this type of equipment must comply with the existing legislation concerning privacy and sensitive information.

## **5.7 Integrated systems**

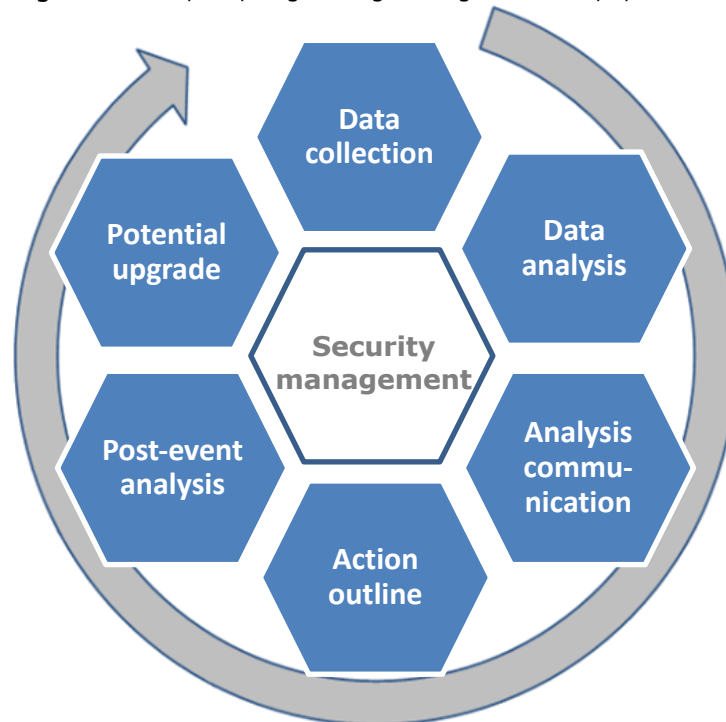
The steady increase in the number and type of commercially available technological security systems that is observed in the last years, is accompanied by heightened complexity and interoperability issues. As a result, there is a high demand for software platforms that are able to successfully manage the information flow from the various interconnected systems and provide the end-user the potential to control everything through a single operating system.

The rising demands in the protection of infrastructures and public spaces have resulted in the simultaneous use of two or more of the previously described systems, that might be created by different manufacturers. Their harmonic cooperation requires an immediate and effective data sharing, which can be performed through an integrated information management system. This specifically developed software is able to easily integrate the different security components, providing all the information in a centralized manner. The use of such systems has a number of advantages including, but not limited to, lower operating costs and personnel demands, faster reaction times, increased efficiency and minimization of false alarms. Moreover, physical security relies regularly on the information provided from IT systems, further highlighting the need for integrated systems.

The assessment and management of the information flow from the different security systems needs to follow certain principles, as shown in Fig. 44. There are several approaches to integrate functions from different

manufacturers into a single software. The principles that are pointed out in the next figure may be considered a first step towards building a robust software that can respond to and efficiently handle a security incident.

**Figure 44.** Main principles governing an integrated security system.



- **Data collection:** Cameras, sensors, access control systems etc., have to share their data with a common system.
- **Data analysis:** The collected data needs to be analysed from the system to assess the criticality and priority of an incident.
- **Analysis communication:** The analysis results needs to be broadcasted to the security operator so as to be confirmed.
- **Action outline:** The system needs to provide an outline of the appropriate actions that need to be performed in order to manage the already confirmed incident.
- **Post-event analysis:** The system needs to store the analysis data and the actions that were followed during an incident in order to facilitate a post-incident analysis by the security officials.
- **Potential upgrade:** Based on the results of the post-event analysis additional functions may have to be added or existing ones may have to be upgraded, which means that the security system needs to allow their integration.

The harmonic integration of different systems is indispensable when dealing with big data, where the information is extracted from huge, often heterogeneous data sets. This is usually the case for information derived from smart city sensors and the Internet of Things, as the data collected through a local security network of a building facility are less complex and extensive. Nevertheless, when the protection of public spaces is of interest, the use of systems that allow for the integration and coordination of different devices and sensors is vital, especially if the analysis has to be performed almost real-time. As an example, FIWARE is an open source cloud platform developed under the initiative of the European Commission in order to provide a space for small and medium size enterprises to make full use of the potential presented by the growth of smart city data and interconnectedness. Still, the convergence of smart city systems and security/surveillance systems is usually challenging due to the different roles and information confidentiality of the city management and law enforcement departments.

## **6 Protection against the malicious use of unmanned aircraft systems**

### **6.1 Introduction**

An unmanned aircraft system (UAS), commonly referred to as 'drone', consists of an unmanned aircraft (also known as unmanned aerial vehicle), the remotely located operator and the components (usually ground control system) through which the communication between those two is achieved. Initially they were constructed and operated within a military context, but their technological advancement, cost reduction and diverse capabilities have led to their extensive use in the civilian domain as they can satisfy the needs of the industry, business and consumer sectors. Many industries have been employing UAS for conducting various activities, including but not limited to, inspections, surveillance, agriculture-related activities, courier services, topographical mapping, marketing, catering and emergency response. Over the last years, the public has been extensively using UAS for recreational purposes as a result of the increased accessibility to a great number of affordable solutions. Beyond visual line of sight (BVLOS) flights that allow a drone to fly beyond visual range and the expansion of 5G networks that support faster data speeds and lower latency are expected to revolutionize the use of drones, while increasing worries regarding security.

The fast proliferation of UAS has raised security concerns, since they can be used by malicious actors, including terrorists and organized crime. Their accessibility, difficult detection, simple and remote piloting make them a valuable tool in the hands of aggressors who can use them to conduct surveillance, spread propaganda, disrupt services or even target assets and people by weaponizing UAS with grenades, CBRN agents or Improvised Explosive Devices (IEDs). Recent examples from around the world demonstrate that UAS are becoming a significant security issue for both public spaces and critical infrastructures, as even off-the-shelf units can be easily transformed into effective weapons and be used intentionally for malicious purposes. Moreover, attention has been brought to the data being generated by the drone use, such as images of critical infrastructures, and whether this information is stored by the UAS manufacturer, thus being exposed to cyberattacks. For instance, certain UAS produced in China have been recently being banned by the US authorities as they failed to meet the 'data management assurance standards' as stated by the US Department of Interior.

Tackling the security threats posed by the use of UAS for terrorist and criminal actions poses several challenges that may be addressed through a combination of different approaches. Some of these approaches include measures that set up a legislative framework regarding pilot licencing, aircraft registration and introduction of flight restricted zones. The latter may be imposed by the employment of geo-awareness and geo-fencing functions, that are pre-installed in the UAS software and alert the operator (geo-awareness) or prevent (geo-fencing) the drone from approaching and entering a sensitive air space (geo-restriction). Clearly, these measures do not offer protection against determined aggressors that may ignore/find ways to circumvent them in order to strike. As a result, there are a number of available countermeasure systems (C-UAS) that incorporate technologies that are able to detect, identify, track and/or intercept a single UAS or a potential 'swarm' attack that exploits multiple drones to accomplish a common objective. Such systems have already been employed in conflict environments, some of which (especially effector-type solutions) cannot be directly used in the urban layout, due to the presence of civilians and other facilities. In this chapter, the current threat from the use of UAS for malicious purposes is presented, followed by an overview of available countermeasures intended for use in the civil domain, underlining the effectiveness and limitations of each system.

### **6.2 UAS categories**

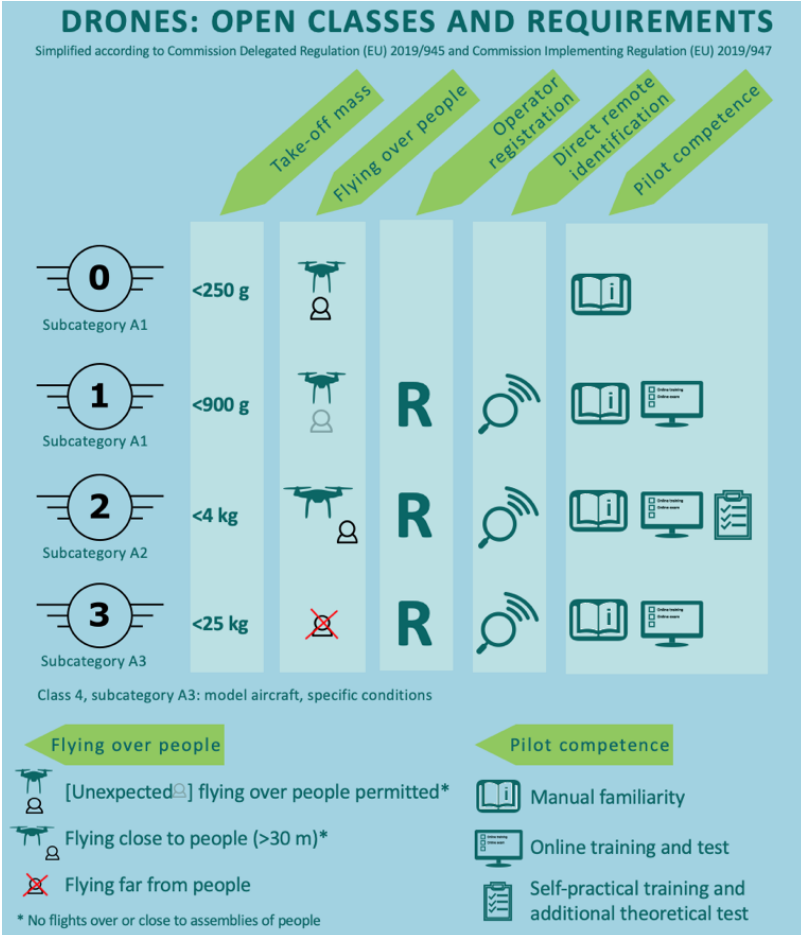
As mentioned before, UAS are used for a variety of different purposes, resulting in different designs depending on the use. When it comes to the protection of a building against UAS non-cooperative intrusions, the design and capabilities of the UAS in the considered attack scenario is of importance, as each countermeasure is rarely effective against all available UAS types. The main UAS categories are the vertical take-off and landing (VTOL) systems and fixed-wing systems, the most popular being the VTOL category which can take-off and land in a vertical manner, having the advantage of a hovering ability and increased capabilities in an urban environment. Each system has a maximum take-off mass (MTOM), that includes its payload capabilities, and depends on its size and motors. The MTOM is a prerequisite for assessing the consequences from an attack with a modified UAS that is transferring an IED, a grenade or a CBRN agent.

The European Commission in 2019 issued two regulations setting out requirements for the design and manufacture of UAS (delegated regulation EU 2019/945) that are intended to be operated under the detailed provisions of (implementing regulation EU 2019/947). In these regulations a UAS classification system is



proposed depending on its MTOM, its maximum attainable speed and the attainable height above take-off point, while detailed operational and technical rules to be followed by manufacturers, operators and Member States are introduced. Fig. 45 presents the UAS ‘open’ category subdivisions as proposed by the abovementioned regulations and the various limits that have to be respected by the operators and manufacturers.

**Figure 45.** UAS open category subdivisions and limits.



**6.3 UAS threats against buildings**

The rapid increase in the availability of UAS and their decreasing cost has not gone unnoticed by terrorist groups, as can be clearly noticed from the rise of the worldwide recorded security-related incidents. Their small size, easy acquisition and modification potential makes them a favourable tool for actors with malicious intent. Terrorist tactics change depending on the target, its vulnerabilities and the motives behind the attack, which means that for selecting effective countermeasures and protecting an asset and its inhabitants, a plethora of different attack scenarios need to be examined. The key threat categories that are relevant for a building facility are:

- **Intelligence, surveillance and reconnaissance:** UAS may be used for gathering information by observing activities with the use of cameras. The increasing capabilities of cameras means that there are units that can operate during night and observe motion through thermal sensors. This method enables aggressors to document a target’s vulnerabilities from a safe distance and exploit them at a later or monitor a target in real-time during an attack. Drones may also be illegally operated from protesters or aggressors to document their actions and the reaction of law enforcement units and use the recording as propaganda material. Information may also be obtained by using powerful microphones that can record confidential conversations.
- **Transfer of hazardous loads:** Easily modified UAS may be used for transferring an IED, grenades or CBRN agents within the building’s security perimeter. Modern UAS are able to carry substantial loads at great distances with increased accuracy through the use of cameras and geographical information

system (GIS) devices. The load can either be placed at a point of interest, be released through a specially designed mechanism or be triggered while in mid-air sacrificing the UAS. The target may be the public (especially if it is outdoors), a specific person (through triggering the payload outside a predetermined office) or the services offered by the structure (e.g. energy, economy, administration, defence).

- **Cyberattacks:** A non-cooperative UAS intrusion may pose a cyber security threat by targeting local wireless networks and disrupting communications, hijacking and/or manipulating sensitive data. A UAS equipped with appropriate gear (such as a network or radio frequency scanner) may easily approach restricted sites and allow hackers to exploit Wi-Fi or Bluetooth network vulnerabilities.
- **Crashing/'kamikaze' attacks:** A UAS, laden with an IED or not, may be piloted with accuracy and deliberately crash on an exposed facility. These 'suicide' or 'kamikaze' drones are usually equipped explosives and may target individuals, structures, networks and communication facilities, serving as an alternative method for substituting ballistic attacks.
- **Jamming:** UAS mounted with electronic equipment may be used to jam perimeter security systems so as to create additional vulnerabilities that can be exploited by the aggressors.
- **Disruption of services/panic reaction:** The presence of the UAS may interfere to the normal operation of an asset due to the safety issues that are raised by such an action, such as interfering with civil aviation in airports. This might also initiate panic reactions from the public leading to injuries and victims or creating favourable conditions for a secondary attack (e.g. channelling people into specific locations).
- **Propaganda:** Protesters and terrorist groups may use UAS to record their actions and use the images for promoting their propaganda. The filmed content may be broadcasted online to encourage other protesters and terrorists and/or recruit new fighters, as it paints the picture of a successful organization with determined members.

## 6.4 Countermeasures

The rapid increase of privately owned UAS, translates in heightened security and safety concerns, leading to intensification of the strive to find effective countermeasures. These countermeasures aim at exploiting the vulnerabilities and shortcomings of available UAS and protect the examined asset. Though, it is pointed out that the technologies described in the current section should be considered as only one of the elements forming the protection strategy against non-cooperative UAS and not the only solution. Other components of this strategy include public awareness campaigns to educate operators on the proper UAS use and the development of routines and protocols that have to be automatically executed by the UAS upon facing certain events. Moreover, intercepting the drone threat is usually easier than identifying and apprehending the operator, which in many cases might prove more valuable as it prevents the individual from performing other similar actions.

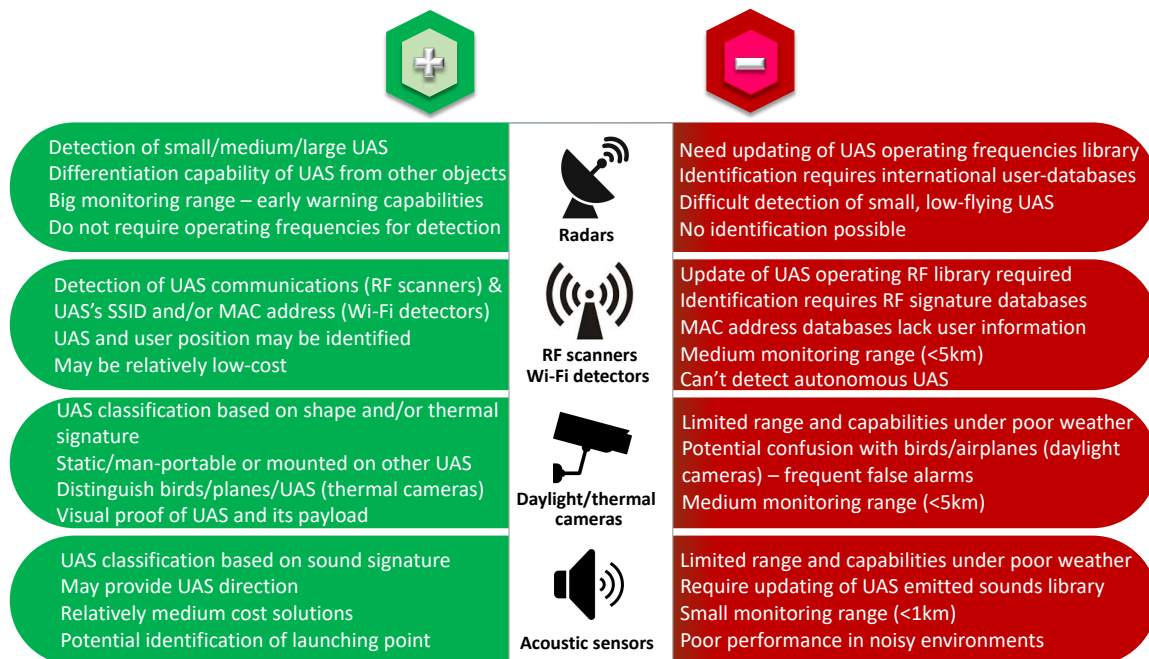
Two broad countermeasure categories may be distinguished, with the first related to systems using sensors to detect, track and identify (DTI systems) incoming UAS, while the second involves kinetic or electronic effectors that are activated to intercept potential drone intrusions. Selecting and deploying the most appropriate C-UAS is a challenging task and requires coherence with the mission assigned to the operating authority and familiarity with the available technologies, their potential and limitations, especially since such solutions are usually extremely high-priced. In an urban setting, these measures are used to secure the airspace around an exposed asset, that might be a building, a monument, a public space or other sensitive facility. Pre-installed UAS software, such as the geo-awareness and geo-fencing functions, pose an alternative method to securing a sensitive air space from unauthorised UAS entrance, even though they are characterised by certain limitations. The adoption of countermeasures that have already been successfully applied for intercepting incoming threats in military conflicts across the globe, is not always recommended in urban areas and crowded places, as they might lead to collateral damage to the population and the facility. As a result, the design of specialized solutions that can be safely used in civilian environments poses one of the greatest challenges in the C-UAS industry.

Several distinct steps (detection, tracking, identification and interception) may be identified in establishing a management framework when dealing with the threat posed by the malicious use of UAS. In each step, specialized countermeasures may be employed; though this implies that responding to the different threat concepts may require the adoption of multiple interlinked systems.

- **Detection, tracking and identification**

Detecting, tracking and identifying incoming UAS poses great challenges, especially in urban environments, as they might be of very small size, while operating at low or high speed and low altitude. For example, systems that depend on UAS speed for detection, e.g. Doppler radars, may prove ineffective if the non-cooperative drone operates at low speed, while in case of high-speed operation, the available timespan for taking decisions (either from the operator or automatically from the employed system) is very short. Detection can be attained by the use of **radar** or **radiofrequency (RF)** scanners that can identify the emitted radio waves. Additionally, **cameras** and **electronic** or **acoustic identification** systems can provide information concerning the UAS size, its potential payload and track its movements. Identifying the drone type, the operator and the departure point of a UAS is certainly more demanding, as the specific visual, acoustic, radar or radiofrequency signature of the UAS needs to be determined. Nearly all available sensor-based systems have certain limitations that need to be considered, before selecting the preferred detection strategy. For instance, discriminating birds from small, low-speed UAS is a challenging process and may cause false alarms, especially if the surveillance airspace is large which means that a large number of birds may be present. Moreover, the radiofrequency of the signal transmitted by the controller (uplink) or the UAS (downlink) may be outside the detection range of the used equipment, especially if the characteristics of the UAS (frequencies and protocols) are not included in the detection equipment's database. In addition, the lack of a comprehensive remote identification system and registration databases signifies that in many cases it might be impossible to identify the operator and match him to the specific non-cooperative UAS. The engagement of multiple sensors may increase detection probability and accuracy, while decreasing uncertainties and false alarms, but this usually comes at a higher purchase cost. Fig. 46 shows some of the most commonly used detection technologies, emphasizing on some of their advantages and limitations.

**Figure 46.** Typical features and limitations of UAS detection/tracking/identification technologies.



- **Interception**

Depending on the information provided from the detection, tracking and identification systems a security operator has to decide on the proper course of action, which may span from doing nothing (in case of a false alarm) to informing the relevant authorities and activating any existing mitigation measures. In case of an attack though, the time period that is available in order to take this decision is very limited. Partly based on experience from military applications, many companies have produced systems that can disrupt a UAS while in flight. The most popular of these kinetic-interception technologies include energy-based weapons (**lasers, high**

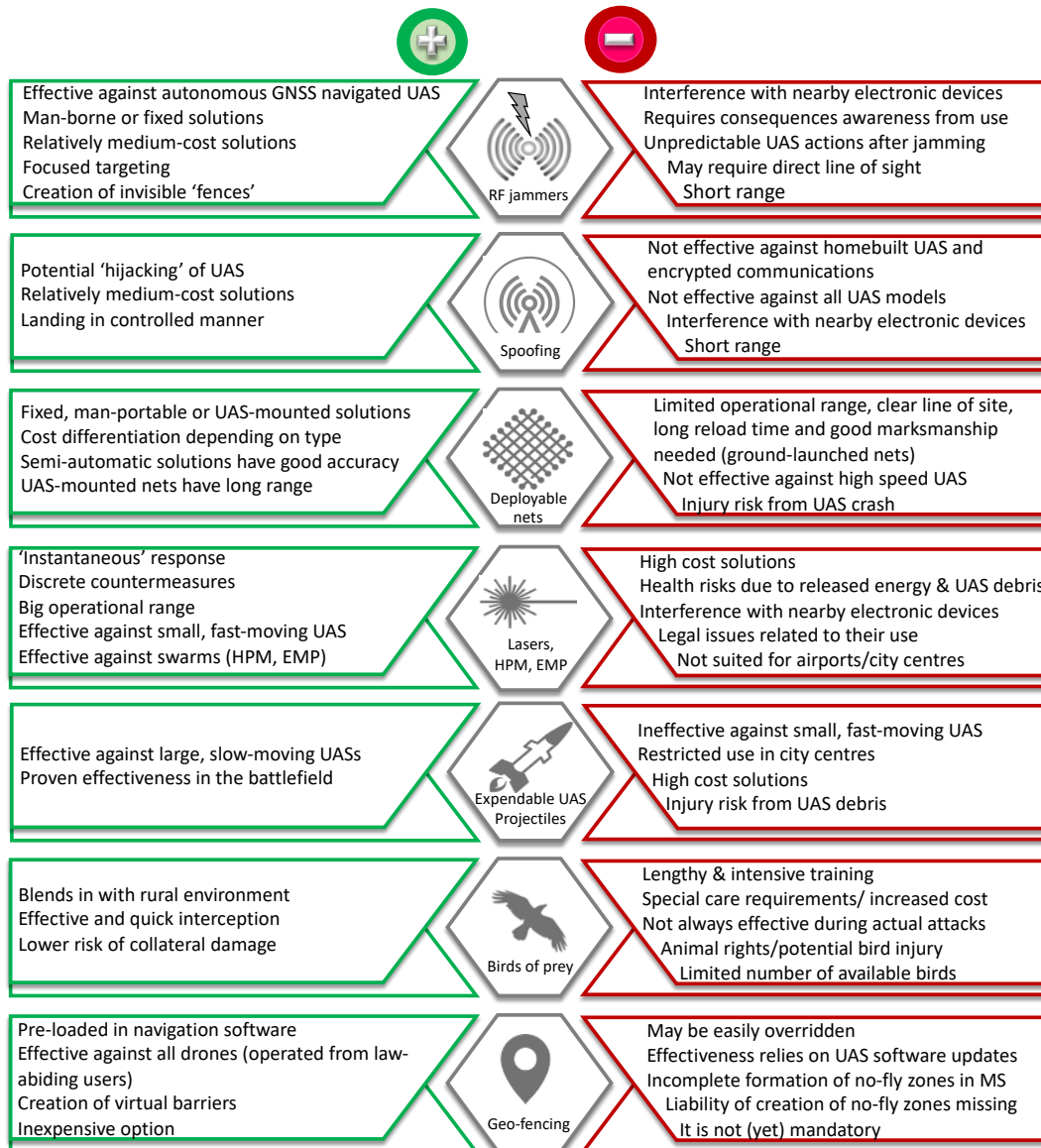
**power microwaves and electromagnetic pulses**) that destroy the body or the electronics of the UAS, **nets** that are launched from the ground or from another UAS, **projectiles** like small missiles similar to those employed in battlefields, **expendable drones** (that may also be equipped with ammunition) that collide with the incoming UAS and **trained birds** (birds of prey) that can grab a UAS while flying. A successful interception of a UAS by employing kinetic-interception technologies usually results in its uncontrolled crash, which may pose a danger to the public, especially in an urban environment.

Non-kinetic interception systems try to minimize the risk of a UAS crash by using technologies that aim to disrupt the communications of the UAS. These include radiofrequency (RF) and global navigation system (GNSS) **jammers** that obstruct the communication between the UAS and either the operator or the satellite link (e.g. GPS) respectively. One major concern during the employment of these systems is the reaction of the UAS once its communication is interrupted, as it might safely land, hover in place or return to its take-off location. Taking control of the UAS by interfering with its communications or navigation link is also the goal of **spoofing**, which allows navigating the drone to safely land or crash.

The most direct approach in protecting an exposed asset from a UAS, even though not an interception technology, is the introduction of a drone 'no-fly' zone through the introduction of an area denial tool at the surrounding airspace (**geo-fencing**). This way, the UAS identification and its intentions becomes less significant since every incoming drone is considered a-priori a threat. Such a procedure is adopted by the majority of civilian airports and critical infrastructure facilities and restricts access to all UAS models. Geo-fencing uses position technologies (e.g. GPS, Wi-Fi, Bluetooth, cellular data) to define the exact location of a UAS and prohibit its entrance to a restricted area. The collection of latitude and longitude points that comprise geo-fenced areas are embedded in the UAS software, which means that it is the responsibility of the UAS manufacturers to update the geofencing data according to the recommendations of the sensitive areas' operators. This usually translates to regular updates that, firstly, manufacturers are not always willing to carry out, and secondly, UAS users have to accept; failure to satisfy these conditions results in ineffectiveness of the geo-fencing technology. Moreover, the restrictions set by geo-fencing can be easily overridden by competent and determined aggressors so as to drive the UAS into sensitive/prohibited areas. EU regulation so far only foresees a geo-awareness system that needs to be implemented in some of the drone subcategories, indicating that the operator will receive a warning when approaching a critical area.

Fig. 47 points out the main advantages and limitations of the above-mentioned interception systems. To overcome the limitations of each individual technology, equipment that combine various elements are available in the market that provide enhanced interception capabilities.

**Figure 47.** Typical features and limitations of UAS interception technologies.



## 6.5 Specific protection measures for buildings

The consideration of UAS as a potential threat for non-military building assets is relatively new, emanating from the great proliferation of such systems in the civil domain. Traditionally, building protection measures focus on attack scenarios, where terrorists try to gain access or cause damage to the facility using ground attacks. The destructive potential of air attacks with the use of UAS and the escalation in autonomous systems has led security officials to take into consideration new attack modus operandi and revise their risk mitigation options.

For efficient building protection against the intrusion of non-cooperative UAS with harmful intentions one has to resort to the development of a holistic protection strategy, where C-UAS technologies are but one element. The first step involves the introduction of physical protection measures and the development of emergency planning and management schemes that can minimize vulnerabilities against UAS attacks (and potentially of other threats). Vulnerabilities that have not been addressed through these measures, may be covered by the installation of one or more of the C-UAS technologies that were described earlier.

The employment of UAS from terrorists, gives them the opportunity to access building areas that were inaccessible during ground attacks, such as interior courtyards, atriums, upper floors and get in proximity to VIP areas. UAS misuse can take various forms, such as being weaponized and strapped with explosives, used for spying and smuggling of items in prisons or other secured facilities, perform cyberattacks and promote propaganda campaigns. The adoption of one or the combination of more of the available countermeasure technologies that were mentioned in the previous section might decrease the risk of an attack against a facility but cannot guarantee protection against the various UAS attack types. Moreover, it is essential to include in the vulnerability assessment of the examined asset additional aspects regarding the surrounding airspace and potential UAS attack scenarios, which are usually ignored during other threats.

One of the main concerns in building security is the threat posed by UAS used as simple and affordable airborne IEDs that can easily approach vulnerable and critical locations within a building's secured perimeter. The payload capacity and the flight range of various UAS models has increased in the last years, following the technological advancements in batteries, electronics and motors. Despite the fact that the size of the explosive device that can be carried by a UAS is still small when compared to other IED transportation means, such as vehicles or suitcases, its ability to quickly and accurately access carefully selected vulnerable locations, makes them a major security threat. To prohibit the entrance of UAS in a building's core (e.g. open-air atrium) and increase the stand-off distance between a potential airborne IED and vulnerable areas, a net in the form of a metal mesh may be employed that covers the exposed area. Such a measure also serves at minimizing the threat from 'kamikaze' attack types and increasing the distance between the UAS and local networks that may pose an attractive target for cyberattacks. The introduction of net-style solutions to protect the façade of a building from a potential contact detonation of an explosive drone is more challenging, so other mitigation solutions are usually adopted. The installation of laminated glass panes at higher floors that can be reachable by UAS may actively mitigate the number of glass fragments produced after the detonation of an explosion device and protect the inhabitants. Façade protection systems also exist that may be placed outside windows and automatically rotate when facing a blast wave, or other similar measures that were described in section 3.8.1. For additional protection, desks may be positioned away from the exterior windows to lower the risk of injuries by the glass fragments that are propelled in the room if an explosion takes place outside the building.

## **6.6 C-UAS integration into the urban environment**

The threats posed from the use of UAS against an asset are characterized by high complexity and diverse attack tactics, requiring balanced decisions from the relevant stakeholders. The risk of using UAS as weapons is deemed as high, attributed to their relatively low cost, direct availability, small size, remote operation and the anonymity of the operator (the EU has already issued regulations to minimize anonymity). The selection of an appropriate C-UAS technology needs to be established after careful consideration of the likelihood of an attack, potential attack scenarios and their parameters, such as the UAS type (e.g. speed, size, range), the surrounding environment (e.g. urban, public space), the potential payload (e.g. explosives, biological agents) and the number of invading UAS (e.g. single or swarm attack). The different aspects of the UAS threat means that a single C-UAS system is simply not capable to respond to all, which results in the employment of layered systems that improve effectiveness and response.

Though, this heightened security comes at a high cost, including the cost of the equipment purchase, maintenance, upkeep and training. C-UAS technologies that have been developed and adopted from European airports to protect their surrounding airspace cost millions, a price-tag that is unbearable for many companies and small enterprises. Manufacturers are already working towards providing more affordable solutions that will also suit smaller business needs and budgets. Alternatives might also be explored, such as leasing C-UAS equipment and operating personnel for periods of heightened security needs (e.g. events) or the installation of relatively cost-efficient measures with different protection levels (e.g. a fixed net at a building's roof to restrict UAS from flying into its open atrium or hardening exterior windows in VIP rooms to mitigate the consequences of a UAS explosive attack).

An asset's perimeter security should be updated to also include UAS threats, as attack tactics that have already been used from terrorist groups outside Europe might be transferred in the urban environment targeting civilians. Selecting tailor-made C-UAS solutions is difficult and requires a thorough investigation of potential attack scenarios. Universal standards and guidelines for rating the performance of C-UAS systems are still missing, so significant differences in their abilities is observed, while their performance might be inferior than advertised. For instance, C-UAS systems intended for providing building perimeter protection in urban layouts, might have been tested and assessed in different conditions, resulting in unexpected operational issues (e.g.

interference with surrounding electronics and communications or projectiles that miss the target due to obstacles).

Non-kinetic interception systems are more adapted for use in city centres, as they avoid the destruction of the UAS that might result in casualties due to the falling debris or the attached IED. As described earlier, these systems rely on jamming the communications between the UAS and the operator or between the UAS and its satellite link or hampering its electronics. Though, one of their major limitations is the danger of interfering with other electronic systems, that are abundant in a city landscape, so their use needs to be carefully examined.

Besides the technological characteristics of the countermeasures that satisfy the security needs of the examined asset, attention needs to be also paid to the legal issues that may be raised before using such systems. The currently existing European regulations focus predominantly on setting rules and restrictions to the UAS use and their operators, while the fragmented landscape results in certain countermeasures being restricted in some Member States, while being admitted in others. The national legislation needs to be considered before investing in a C-UAS technology and ascertain whether the intended C-UAS use in the specific environment and from the specific user is legal.

## **6.7 Threats from other types of unmanned vehicles**

The current chapter is dedicated to the threats posed from the malicious use of UAS, mainly focusing on the consequences after potential attacks and the availability of countermeasures that may be employed to respond to such incidents. However, other type of unmanned vehicles may also be exploited to approach sensitive facilities with malicious intent. For instance, a driverless car or van may be used to carry a vehicle-borne improvised explosive device (VBIED) close to target or to perform a vehicle ramming attack. Similarly, autonomous ships and vessels may be used to attack other ships or facilities that are adjacent to the sea, riverbeds or lakes and lack proper security measures. Given the rapid technological advancements in the field of autonomous vehicles and the preference of aggressors to strike while being invisible, such attacks may proliferate in the near future. The ability to remotely control a vehicle minimizes the need of terrorist groups to recruit new members, as the difficulties in detecting, identifying and apprehending the remote operator increase the chances of a successful escape. This implies that the risk of terrorist attacks against sensitive facilities might increase, as the prospect of avoiding arrest makes such attacks more attractive.

Many C-UAS technologies that were described earlier may also provide solutions against unmanned vehicles other than aircrafts, though they may not be specifically designed for them. Clearly, physical protection measures that are used to harden facilities against terrorist threats, e.g. the employment of protective barriers to prohibit unauthorised vehicle entrance, are also effective against unmanned vehicles. Though, automated or semi-automated vehicles pose unique challenges in the security domain, since disabling the driver, and consequently the vehicle, is not an option. Such threats are bound to become more common due to the advancement of unmanned technologies and need to be addressed by security managers during the development of their asset's protection strategy. Finally, maintaining increased awareness is a prerequisite for a meaningful and systematic review of the relevant risk so as to consider emerging threats and technologies that may be misused by terrorists, such as those of unmanned vehicles.

## 7 Concluding remarks

The current guideline has sought to underline the need for both state and private stakeholders to update their strategy on building perimeter protection, especially in response to emerging threats and challenges arising from the great technological advancements of the modern era. A number of different threats against the building infrastructure and linked to the risk of terrorism have been collected, adapted and presented in this report, focusing on the principles that guide the selection and installation of protection solutions. As has been highlighted in many parts, a reliance on a sole protection measure is highly unlikely to safeguard against all the presented attack scenarios. Consequently, it is imperative to develop of a comprehensive protection strategy that will effectively integrate the different protection technologies within a broad multi-threat framework.

A holistic protection planning, followed by a multidimensional response, needs to commence with an asset-specific risk assessment that draws together various terrorism-related data and provides tailor-made suggestions for reducing the risk of a terrorist attack. Prior incidents may provide valuable information regarding the likelihood of an attack and prevailing attack tactics, while assessing the vulnerabilities of the examined site can reveal the consequences if an attack materializes. Despite the fact that zero risk is impractical in both technical and economic terms, a carefully considered, thorough and well-balanced protection plan will substantially reduce the risk posed from a terrorist attack against a building structure.

A methodology for the calculation of external explosion loads that need to be considered in the blast protection design of a structure has been presented. Thus, several formulas, graphs and diagrams have been included, which make this guide sufficiently self-contained, especially for relatively simple cases of blast loading. Various techniques for the protection of structures against external and internal explosive loads have been introduced which are of particular interest for vulnerable areas, such as access control zones and other freely accessible building locations. Moreover, to minimize the likelihood of the development of a progressive collapse mechanism, design considerations have been included, such as the reinforcement of key structural elements and promotion of structural robustness techniques.

Protection against attacks with the use of vehicles, that are used to either ram into crowded places or to transfer an explosive device close to a facility, can be accomplished by implementing a hardened perimeter. Physical protection measures around buildings and critical infrastructures restrict unauthorised vehicle access and enforce a minimum stand-off distance between the building façade and the potential IED. Within this guide an approach for the selection of simple, tailor-made and effective perimeter protection measures has been exhibited, focusing on measures that can be harmonically integrated to the surrounding environment according to a security-by-design concept. This means that security measures can be embedded into innovative architectural and artistic concepts, without sacrificing their impact performance and stopping power.

Digital advancements can also facilitate building security by employing state-of-the-art technologies, such as video surveillance, intruder detection, smart sensors, access control and video analytics. These systems can significantly enhance the security of vulnerable sites through harnessing and analysing incoming data, predicting states of emergency and guaranteeing quick response in case of an incident. Intelligent video surveillance systems and smart sensors bring security breaches directly to the attention of security officials minimizing reaction time and therefore mitigating potential consequences. The integration of different building perimeter security systems into one software platform results in increased effectiveness and lower administration, training and maintenance cost. This cooperation of various security components under a single and flexible system is usually complex and characterized by interoperability issues, requiring immediate data sharing and standardized interfaces and protocols that in some cases are still missing.

Building perimeter protection planning needs to include techniques that enhance conventional security measures, so as to respond to the novel threat landscape, such as the misuse of UAS. To counter these complex and rapidly evolving threats one has to prepare for terrorist tactics that were not considered in the past and respond dynamically by investing in innovative countering tools. Careful consideration is required when selecting counter technologies, as legal restrictions and lack of common testing protocols may result in operational constraints and ineffectiveness respectively. The preferred response to the multifaceted threat of UAS depends greatly on the operating environment, the location of the examined facility and the legal and regulatory frameworks set in each Member State. Moreover, artificial intelligence and automation are quickly transforming the threat landscape creating new security challenges that call for continuous monitoring of technological developments both in a 'malicious use' (attacking vulnerable facilities) and a countering (providing practical countermeasures) concept.



The material presented can help for introducing the subject of building physical security, and in most cases can form a basis allowing the development of a reliable protection strategy. This is important for security officers and engineers, as in many cases this information is fragmented and not yet managed in an orderly manner.

## References

- Aleem U., Furqan A., Heung-Woon J., Sung-Wook K., Jung-Wuk H., *Review of analytical and empirical estimations for incident blast pressure*, KSCE Journal of Civil Engineering, DOI: 10.1007/s12205-016-1386-4, 2016.
- American Society for Testing and Materials, *ASTM F 2656, Standard Test Method for Vehicle Crash Testing of Perimeter Barriers*, United States, 2018.
- American Society for Testing and Materials, *ASTM F 1642M, Standard Test Method for Glazing and Glazing Systems Subject to Airblast Loadings*, United States, 2017.
- American Society of Civil Engineers, ASCE, *Blast Protection of Buildings*, American Society of Civil Engineers, 2011.
- American Society of Civil Engineers, ASCE, Petrochemical Committee, Task Committee on Blast Resistant Design, *Design of Blast Resistant Buildings in Petrochemical Facilities*, American Society of Civil Engineers, New York, 1997.
- American Society for Testing and Materials, *ASTM F 1642, Standard Test Method for Glazing and Glazing Systems Subject to Airblast Loadings*, United States, 2017.
- Arrigoni M., Bedon C., van Doormaal A., Haberacker C., Husken G. et al., *Suggestions for adaptations of existing European Norms for testing the resistance of windows and glazed facades to explosive effects*, JRC Technical Report, Joint Research Centre, Internal use only, JRC107655, 2017.
- Baker W. E., Cox P. A., Westine P.S., Kulesz J.J., Strehlow R.A., *Explosion Hazards and Evaluation*, Elsevier, Amsterdam, 1983.
- Bedon C., van Doormaal A., Haberacker C., Husken G., Larcher M., *Recommendations for the Improvement of Existing European Norms for Testing the Resistance of Windows and Glazed Facades to Explosive Effects*, European Union Publication Office, EUR 27554 EN, ISBN-13:978-92-79-53394-5, 2015.
- Berger J., Heffernan P., Wight G., *Blast testing of CFRP and SRP strengthened RC columns*, Structures Under Shock and Impact X, 95-104, 2008, <https://doi.org/10.2495/SU08010.1>
- Bogosian D., Ferritto J., Shi Y., *Measuring uncertainty and conservatism in simplified blast models*, AD-B082 713, 30th explosives safety seminar, Atlanta, GA, 13–15 August, 2002.
- British Standards Institution, *PAS:68, Impact test specifications for vehicle security barrier systems*, UK, 2013.
- CEB, *Concrete Structures under Impact and Impulsive Loading*, Comite Euro-International du Beton, Bulletin d'Information, No. 87, Lausanne, Switzerland, 1988.
- Centre for the Protection of National Infrastructure, CPNI EBP 10/13, *Guidance note: Peel Adhesion Testing and Assessment of Anti-shatter Film (ASF)*, 2013.
- Control Risks Group Holdings Ltd, 2018, < <https://www.controlrisks.com/>>.
- Coursey B., Mattson P., Kourti N., Puskar E., Bilotte E., Marshall J., Karam L., *Standard Practice*, 2016, CBRNE World, San Diego, California, USA.
- European Commission, *The European Agenda on Security*, COM(2015) 185, Brussels, 2015.
- Cranz C., *Lehrbuch der Ballistik*. Berlin: Springer, 1926.
- Defence Advanced Research Projects Agency (DARPA), Chemical and Biological Sensor Standards Study II, Department of Defence (DoD), Washington DC, 2010.
- Dusenberry D., *Handbook for Blast-Resistant Design of Buildings*, John Wiley & Sons, INC. New Jersey, USA, 2010.
- Eibl J., *Soft and Hard Impact. Concrete for Hazard Protection*, Concrete Society, Edinburgh, UK, p. 175-186, 1987.
- European Commission, *Action Plan to support the protection of public spaces*, COM(2017) 612, Brussels, 2017a.
- European Commission, *Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks*, COM 610/2017 (<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017DC0610>)

European Commission, Commission Staff Working Document, *Overview of Natural and Man-made Disaster Risks the European Union may face*, SWD (2017), Brussels, doi: 10.2795/861482, 2017b.

European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy, COM 605/2020 ( <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605> )

European Commission Joint Research Centre, *Europe Media Monitor*, 2020, < <http://emm.newsbrief.eu/overview.html>>.

European Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.

European Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

European Committee for Standardization (CEN), *Eurocode 0: Basis of Structural Design*, EN 1990, 2005

European Committee for Standardization (CEN), *Eurocode 1: Actions on Structures*, EN1991, 2001.

European Committee for Standardization (CEN) Eurocode 1: Actions on structures, Part 1-7: prEN 1991-1-7: *General actions-Accidental actions*, 2006.

European Committee for Standardization (CEN), EN 12600, *Glass in building - Pendulum test - Impact test method and classification for flat glass*, 2002.

European Committee for Standardization (CEN), EN 356, *Glass in building – Security glazing – Testing and classification for resistance against manual attack*, 1999.

European Committee for Standardization (CEN), EN 1063, *Glass in building – Security glazing – Testing and classification of resistance against bullet attack*, 1999.

European Committee for Standardization (CEN), EN 13123-1, *Windows, doors and shutters – Explosion Resistance – Requirements and classification – Part 1: Shock tube*. 2001.

European Committee for Standardization (CEN), EN 13123-2, *Windows, doors and shutters – Explosion Resistance – Requirements and classification – Part 2: Range test*, 2004.

European Committee for Standardization (CEN), EN 13541, *Glass in building – Security glazing – Testing and classification of resistance against explosion pressure*, 2012.

European Committee for Standardization, *CWA16221, Vehicle security barriers-performance requirements, test methods and guidance on application*, 2010.

European Data Protection Board (EDPB), *Guidelines 3/1029 on processing of personal data through video devices*, 2019.

FM Global 1-44, *FM Global Property Loss Prevention Data Sheets, Damage-Limiting Construction*, Johnston RI, 2012.

General Services Administration (GSA), *Progressive collapse Analysis and Design Guidelines for New Federal Buildings and Major Modernization Projects*, U.S. General Services Administration, Washington DC, 2013.

Goel M., Matsagar V., Gupta A. et al., *An abridged review of blast wave parameters*, Defence Science Journal, Vol. 62(5), p.300-306, 2012.

GSA TS01, “Standard Test Method for Glazing and Window Systems Subject to Dynamic Overpressure Loadings”, US General Services Administration, 2003.

Hopkinson B., *British Ordnance board minutes* No. 13565. p. 220, 1915.

IHS Markit, *Jane’s 360- Defence & Security Intelligence & Analysis*, 2018 < <https://www.janes.com/>>

Interagency Security Committee (ISC), *The Risk Management Process for Federal Facilities*, Department of Homeland Security, USA, 2016.

International Ammunition Technical Guideline (IATG), *Formulae for ammunition management 01.80*, United Nations, 2011.

International Organization for Standardization, ISO16933, *Explosion Resistant security glazing-test and classification for Arena air-blast loading*, Vernier, Switzerland, 2007.

International Organization for Standardization, ISO 31000: *Risk management – Principles and guidelines*, 2009.

International Organization for Standardization, ISO 31010: *Risk management – Risk assessment techniques*, 2018.

International Organization for Standardization, *Vehicle Security Barriers-Part 1: Requirement, Vehicle impact test method and performance rating*, IWA 14-1, Vernier, Switzerland, 2013.

International Organization for Standardization, *Vehicle Security Barriers-Part 2: Application*, IWA 14-2, Vernier, Switzerland, 2013.

Karlos V., Larcher M., Solomos G., *Guideline: Selecting proper security barrier solutions for public space protection*, EUR 113778, European Commission, Ispra, Italy, 2018. (Available on request by the authors)

Karlos V., Solomos G., Larcher M., *Analysis of the blast wave decay coefficient using the Kingery-Bulmash data*, International Journal for Protective Structures, Vol. 7(3), p. 409-429, 2016.

Kingery C. N., Bulmash G., *Technical report ARBRL-TR-02555: Air blast parameters from TNT spherical air burst and hemispherical burst*, AD-B082 713, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, 1984.

Krauthammer T., Altenberg A., *Negative phase blast effects on glass panels*, International Journal of Impact Engineering, Vol. 24(1), p. 1-17, 2000.

Larcher M., *Security in Public Spaces*, < <https://www.mrrb.bg/en/pts-security-in-public-spaces-martin-larcher-soft-target-public-spaces-vulnerability-assessment-and-protection/>>, 2018.

Larcher M., Solomos G., Casadei F., Gebbeken N., *Experimental and numerical investigation of laminated glass subjected to blast*, International Journal of Impact Engineering, Vol. 39, pp. 42-50, 2012.

National Fire Protection Association, NFPA 68, *Standard on Explosion Protection by Deflagration Venting*, Quincy MA, 2018.

Pachman J., Matyas R. and Kunzel M., *Study of TATP: blast characteristics and TNT equivalency of small charges*, Shock Waves, Vol, 24, Is. 4, p. 439-445, 2014.

Prevention Web, 2018, *Sendai Framework for Action on Disaster Risk Reduction 2015-2030* < <https://www.preventionweb.net/drr-framework/sendai-framework-monitor/indicators>>

University of Maryland, Global Terrorism Database, 2018 < <https://www.start.umd.edu/gtd/>>

Remennikov A., Mentus I., Uy B., (2015) “Explosive breaching of walls with contact charges: Theory and Applications”, International Journal of Protective Structures, Vol.6, No. 4, p. 629-647, 2015.

Rigby PD., Tyas A., Bennett S., Clarke S., Fay S., *The negative phase of the blast load*, International Journal of Protective Structures, Vol. 5(1), p.1-20, 2014.

Shin J., Whittaker AS., Cormie D., Incident and normally reflected overpressure and impulse for detonations of spherical high explosives in free air, journal of Structural Engineering, DOI: 141:04015057, 2015.

Smith PD., Hetherington JG., Shi Y., *Blast and Ballistic Loading of Structures*, London: Butterworth-Heinemann Ltd 1994.

Solomos G., Larcher M., Valsamos G., Karlos V., Casadei F., *A survey of computational models for blast induced human injuries for security and defence applications*, JRC Technical Reports, European Commission, Ispra, Italy, 2020, ISBN 978-92-76-14659-9, doi: 10.2760/685, JRC119310.

Teich M., Gebbeken N., *The influence of the underpressure phase on the dynamic response of structures subjected to blast loads*, International Journal of Protective Structures, Vol. 1(2), p.219-233, 2010.

Unified Facilities Criteria, *UFC 3-340-02 Structures to Resist the Effects of Accidental Explosions*, U.S. Army Corps of Engineers, Naval Facilities Engineering Command, Air Force Civil Engineer Support Agency, 2008.

Unified Facilities Criteria, *UFC 4-023-03 Design of Building to Resist Progressive Collapse*, U.S. Army Corps of Engineers, Naval Facilities Engineering Command, Air Force Civil Engineer Support Agency, 2016.

U.S. Department of the Army, *Design and Analysis of Hardened Structures to Conventional Weapons Effects*, Technical Manual 5-855-1, 1997.

U.S. Department of the Army, *Structures to resist the effects of accidental explosions*, Technical Manual 5-1300, 1990.

Valsamos G., Larcher M., Casadei F. Karlos V., *A numerical framework to support the certification of barrier testing*, EUR 30165 EN, European Commission, Ispra, 2020, ISBN 978-92-76-17856-9 , doi:10.2760/797952 , JRC120307

Vapper M., Lasn K., *Blast protection of concrete columns with thin strips of GFRP overlay*, Structures, Vol. 25, 491-499, 2020.

Verein Deutscher Ingenieure e.V., VDI 3673, *Pressure Release of Dust Explosions*, Guideline VDI 3673, VDI-Verlag Dusseldorf, Germany, 2002.

## List of abbreviations and definitions

AN	Annealed Glass
ASF	Anti-Shatter Film
ASCE	American Society of Civil Engineers
ASTM	American Society for Testing and Materials
BSI	British Standards Institute
CBRN	Chemical, Biological, Radiological and Nuclear
CCTV	Closed-Circuit Television
CEN	European Committee for Standardization
CPNI	Centre for the Protection of National Infrastructure
C-UAS	Countermeasures for Unmanned Aircraft Systems
DTI	Detect, Track and Identify
EC	European Commission
EMM	European Media Monitor
ERNICIP	European Reference Network for Critical Infrastructure Protection
EVA	Ethylene-Vinyl Acetate
EU	European Union
FT	Fully tempered or Toughened Glass
GIS	Geographical Information System
GNSS	Global Navigation System
HD	High Definition
HS	Heat-strengthened Glass
ICCD	Intensified Charge-coupled device
IED	Improvised Explosive Device
ISC	Interagency Security Committee
ISO	International Organizations for Standardization
JRC	Joint Research Centre
MTOM	Maximum Take-off Mass
NRA	National Risk Assessment
PBIED	Person borne improvised explosive device
PVB	Polyvinyl-Butyral
RDD	Radiological Dispersion Devices
RF	Radiofrequency
TNT	Trinitrotoluene
UAS	Unmanned Aircraft System
UFC	Unified Facilities Criteria
VBIED	Vehicle borne improvised explosive device
VIP	Very Important Person
VTOL	Vertical Take-off and Landing

## List of figures

<b>Figure 1.</b> Global terrorism threat level in 12/2019-05/2020 by JRC terrorism database using EMM. (Background map © Mapbox, © OpenStreetMap). .....	7
<b>Figure 2.</b> Fatalities per month from Global Terrorism Database (1970-2017, year 1994 is missing in the recordings) and Control Risks (2018-2019). .....	9
<b>Figure 3.</b> Risk assessment process. ....	10
<b>Figure 4.</b> Worldwide terrorist attacks by a) utilized modus operandi and b) target. ....	11
<b>Figure 5.</b> Threat level from terrorist attacks in central Africa and Middle East in 12/2019-03/2020 by JRC terrorism database using EMM. (Background map © Mapbox, © OpenStreetMap).....	12
<b>Figure 6.</b> Indicator point system for assessing criticality of exposed assets. ....	15
<b>Figure 7.</b> Risk administration options. ....	17
<b>Figure 8.</b> Risk and protective design reviewing diagram. ....	19
<b>Figure 9.</b> Types of external unconfined explosions: (a) Free-air burst, (b) Air burst, and (c) Surface burst. ...	20
<b>Figure 10.</b> Upper charge mass limit per mean of transportation. ....	21
<b>Figure 11.</b> Peak reflected pressure and reflected impulse versus stand-off distance.....	22
<b>Figure 12.</b> Incident and reflected pressure time histories. ....	27
<b>Figure 13.</b> Parameters of positive phase of shock spherical wave of TNT charges from free-air bursts (modified from UFC 3-340-02, 2008). ....	29
<b>Figure 14.</b> Parameters of negative phase of shock spherical wave of TNT charges from free-air bursts (modified from UFC 3-340-02, 2008). ....	30
<b>Figure 15.</b> Parameters of positive phase of shock hemispherical wave of TNT charges from surface bursts (modified from UFC 3-340-02, 2008). ....	31
<b>Figure 16.</b> Parameters of negative phase of shock hemispherical wave of TNT charges from surface bursts (modified from UFC 3-340-02, 2008). ....	32
<b>Figure 17.</b> Formation of Mach front and triple point due to a near ground explosion.....	33
<b>Figure 18.</b> Estimation of Mach front height $H_T$ from the scaled charge height $H_c/W^{1/3}$ and scaled horizontal distance $H_G/W^{1/3}$ . ....	33
<b>Figure 19.</b> Angle of incidence at a building face. ....	34
<b>Figure 20.</b> Influence of the angle of incidence on the ratio of reflected to incident overpressure (modified from UFC 3-340-02, 2008).....	35
<b>Figure 21.</b> Influence of the angle of incidence on the positive reflected impulse (modified from UFC 3-340-02, 2008). ....	35
<b>Figure 22.</b> Sketch of a typical Pressure-Impulse diagram. ....	37
<b>Figure 23.</b> Glass ratings under arena testing (modified from ISO 16933 and ASTM F1642M). ....	41
<b>Figure 24.</b> Failure mechanism of laminated glass. ....	42
<b>Figure 25.</b> Protective blast walls.....	47
<b>Figure 26.</b> Blast wave pressure distribution [Pa] for the ‘open door’ case (upper images) and the ‘meandering’ case (lower images) at 4ms and 10ms after detonation. ....	48
<b>Figure 27.</b> Typical design of blast release vents. ....	49
<b>Figure 28.</b> Partial collapse of Alfred P. Murrah Federal building [FEMA, 1995]. ....	50

<b>Figure 29.</b> Strategies for accidental design situations (EN1991-1-7, 2006).....	51
<b>Figure 30.</b> Blast protective measures design process. ....	55
<b>Figure 31.</b> Selection approach for anti-ramming vehicle barrier selection. ....	56
<b>Figure 32.</b> 2D and 3D satellite image of an area containing a potential target [OpenStreetMaps, Google Earth] .....	57
<b>Figure 33.</b> Vehicle modes of impact. ....	58
<b>Figure 34.</b> Laden weight per vehicle type. ....	59
<b>Figure 35.</b> Vehicle modes of impact. ....	60
<b>Figure 36.</b> Typical protective bollards.....	61
<b>Figure 37.</b> Typical temporary protective barriers.....	62
<b>Figure 38.</b> Typical street furniture elements. ....	62
<b>Figure 39.</b> Typical landscape protective solutions. ....	63
<b>Figure 40.</b> Advantages and disadvantages of passive barrier solutions.....	63
<b>Figure 41.</b> Typical active barriers. ....	64
<b>Figure 42.</b> Advantages and disadvantages of active barrier solutions. ....	65
<b>Figure 43.</b> Examples of innovative protective barriers.....	65
<b>Figure 44.</b> Main principles governing an integrated security system. ....	77
<b>Figure 45.</b> UAS open category subdivisions and limits. ....	79
<b>Figure 46.</b> Typical features and limitations of UAS detection/tracking/identification technologies. ....	81
<b>Figure 47.</b> Typical features and limitations of UAS interception technologies. ....	83



**List of tables**

**Table 1.** Soft target categories. .... 13

**Table 2.** Scoring criteria per indicator. .... 16

**Table 3.** Assessment of an asset’s criticality. .... 16

**Table 4.** Equivalence TNT factors (various sources). .... 24

**Table 5.** Deformation criteria for blast-induced elements (modified from ASCE, 2011). .... 39

**Table 6.** Classification for glazing resistance to impact. .... 42

**Table 7.** Classification for glazing resistance to manual attacks. .... 43

**Table 8.** Classification for glazing resistance to armed attacks. .... 43

**Table 9.** Classification for glazing resistance to explosive attacks. .... 44

**Table 10.** Classification for window system resistance to explosive attacks. .... 44

**Table 11.** Suggestions during the analysis of structures against progressive collapse according to different standards. .... 53

**Table 12.** Design load combinations for building progressive collapse analysis. .... 54

**Table 13.** Specifications for vehicle security barrier impact assessment. .... 66

**Table 14.** Abbreviations for barrier performance ratings. .... 66

**Table 15.** Vehicle classes and relevant weight. .... 67

**Table 16.** Vehicle kinetic energy [kJ]. .... 68

**Table 17.** Reference point locations and penetration rating. .... 69

**Table 18.** Video surveillance considerations. .... 73

**Table 19.** Video analysis algorithm types. .... 74

**Table 20.** Effect of access control types on vehicle transit time. .... 75



## **GETTING IN TOUCH WITH THE EU**

### **In person**

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

### **On the phone or by email**

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by electronic mail via: [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)

## **FINDING INFORMATION ABOUT THE EU**

### **Online**

Information about the European Union in all the official languages of the EU is available on the Europa website at: [https://europa.eu/european-union/index\\_en](https://europa.eu/european-union/index_en)

### **EU publications**

You can download or order free and priced EU publications from EU Bookshop at: <https://publications.europa.eu/en/publications>. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see [https://europa.eu/european-union/contact\\_en](https://europa.eu/european-union/contact_en)).

## The European Commission's science and knowledge service

Joint Research Centre

### JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



**EU Science Hub**  
[ec.europa.eu/jrc](https://ec.europa.eu/jrc)



@EU\_ScienceHub



EU Science Hub - Joint Research Centre



EU Science, Research and Innovation



EU Science Hub

