FP 7 SPIRIT Project concerning Infrastructure Protection

Ans van Doormaal, Jaap Weerheijm, Frank van het Veld, and Bart Boonacker

TNO
P.O. Box 45, 2280 AA Rijswijk, The Netherlands

Abstract

SPIRIT is an acronym for Safety and Protection of built Infrastructure to Resist Integral Threats. Within the 7th framework of the EU, the SPIRIT consortium was formed to bring the required expertise regarding protection of infrastructure against terrorist threats together, to make these commonly available and to find solutions that can be integrated into normal life and planning and building procedures. SPIRIT addresses CBRE terrorist attack scenarios. The anticipated main outcome of the project is an integrated approach to evaluate and counter CBRE-threats, including proposed guidelines for an EU Regulatory Framework. With this approach, government, end users of buildings and designers can define and achieve a desired level of protection.
Keywords: Countermeasures, protection, vulnerability, infrastructure, CBRE threats

1 Introduction

Terrorist attacks by bombing (E) or Chemical, Biological or Radiological (CBR)-agents are threats with a low probability but with disastrous consequences. There is strong need to protect people, the societal community and critical infrastructures and utilities against being damaged, destroyed or disrupted by deliberate acts of terrorism. Solutions have to be developed to realize sufficient resilience of the urban infrastructure for rare occasions with minimum effect on normality. Hitherto, normal regulations and building guidelines do not take into account the CBRE threat.

Within the 7th framework of the EU, the SPIRIT (Safety and Protection of built Infrastructure to Resist Integral Threats) consortium was formed to bring the required expertise together, to make these commonly available and to find solutions that can be integrated into normal life and planning and building procedures. The consortium is a collaboration between several European government organizations, academic institutions and companies (see Figure 1.1). TNO is the coordinator.

Figure 1.1: The SPIRIT-consortium

The aim of the project is to develop an integrated approach to mitigate Chemical, Biological, Radiological and Explosive threats to built infrastructure and to propose guidelines for an EU Regulatory Framework. SPIRIT started in August 2010 and is due to conclude and report to the European Commission by the end of 2013. This paper gives an overview of the project.

2 Scope, objectives and work packages

The scope of the SPIRIT-project is defined by the type of threats and the type of built infrastructure considered. The threats considered are terrorist threats with use of CBRE-means. Regarding the infrastructural target, we limit ourselves to large modern buildings, often (partly) public buildings, where a lot of people can be present. Modern refers to the fact that only buildings are considered that are designed according to the current standards.

The targeted contribution of SPIRIT to built infrastructure protection will be:
- A methodology to quantify the vulnerability of built infrastructure in number of casualties/injuries, amount of damage and loss of functionality and services;
- A guidance tool to assess the vulnerability of a design/building and select efficient and cost effective countermeasures (ready to use solutions) to achieve a required protection level against terrorist attacks;
- Portfolios of protection products for new and existing buildings;
- Recommendations for draft EU regulatory framework to enable safety based engineering and the incorporation of 'CBRE protection' in the regular building guidelines and regulations.

The technical work of the SPIRIT project is divided in five work packages. Figure 2.1 shows these work packages, as well as the interrelation between them.

Figure 2.1: Overall strategy of SPIRIT

3 Threat assessment and scenarios

Within the SPIRIT project, scenarios are defined which are specific for attacks on buildings. In total, 20 Chemical, 12 Biological, 9 Radiological and 14 Explosive scenarios have been defined [1].

To be able to make a well-considered choice of the vast amount of available CBR agents, some new concepts are introduced like 'building interaction vectors' and a 'threat space' [2]. Interaction vectors describe how a building interacts with the outside world. Examples of interaction vectors are shown in Figure 3.1. By exploiting these interaction vectors, one can get an indication about how a building can be attacked. Also, by reciprocating safety principles (how can I make things go wrong?) additional attack possibilities are defined.

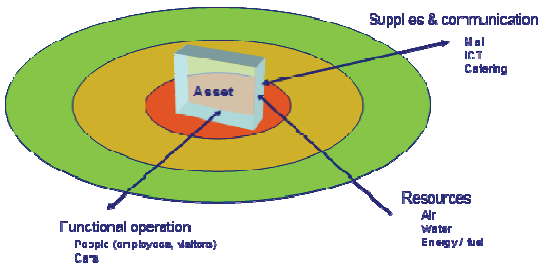

Figure 3.1: Examples of interaction vectors and carriers of a building with the outside world, that can possibly be exploited as attack vectors

A CBR threat space is a (visual) representation of agents in a multidimensional space to ensure that the threat has been evenly distributed through the threat spectrum, avoiding clustering around 'known' (already happened/studied in the past) attacks which may cause bias. By superimposing scenarios that have occurred in the past or are considered to be credible in other studies, some 'blind spots' are identified in the interaction vector exploits, i.e. an exploited vector could theoretically be used for an attack on a building, however no occurred or credible scenarios were (yet) found in existing literature. Finally a set of 41 attack scenarios were defined to represent all different CBR attacks.

For explosive attacks, a range of explosive materials are known to have been used in actual terrorist attacks. However, the well established procedure of TNT-equivalence has been adopted to define representative quantities of high explosives and credible scenarios. In the framework of infrastructure safety, (close-in) blast is assumed to be the dominant phenomenon to be considered in this study, whereas fragments from either casing around or shrapnel in the explosive charge cause effects of second order. Therefore the TNT-equivalency-approach is appropriate.

4 Incident analysis

It is a challenge to develop a relatively simple, not too detailed consequence analysis methodology for the guidance tool, that still has the ability to discern between different cases, scenarios and buildings, and that also can show the effectiveness of protective measures.

The anticipated approach is a kind of three dimensional database method, with a bypass, where possible, based on simple quantitative correlations. The three dimensions are threat classes, a categorization of the structures and structural elements, and consequence classes, in terms of structural damage, injuries and/or loss of functionality.

The quantitative breakdown will be based on a large number of calculations, both with relatively simple engineering tools, as well as with sophisticated numerical tools, e.g. for analyzing specific details. These analyses are done to understand the phenomena that are dominant for the consequences and to select the proper parameters to consider in the tool.

Two generic buildings, that have been defined, are the target constructions for the analyses to be performed: a multi-use high rise concrete frame structure and a large shopping mall of prefabricated elements. The consequence calculations concern blast loading calculations, window breakage analysis, damage zone prediction, injury and lethality prediction, column damage due to close-in charges and residual capacity, analysis of progressive collapse, the dispersion of CBR-agencies through the building and the CBR-lethality. Figure 4.1 shows some examples.

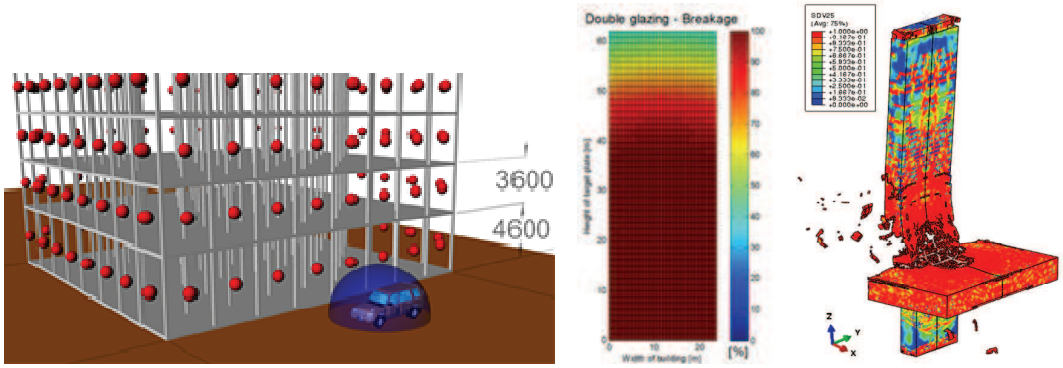

Figure 4.1: Examples of incident analysis; a. car bomb, b. glazing failure and hazard along building façade, c. column damage due to close-in detonation

5 Protective measures

Protective products will be identified and developed in order to provide architects and building designers with ready-to-use products and solutions to harden infrastructure against CBRE terrorist threats. The innovative products for protection of structural components and indoor air quality are related to the identified CBRE-threats. Countermeasures such as blast proof masonry retrofit systems, blast resistant window/facade systems, micro-reinforced high performance concrete, detectors, monitors and filters for ventilation systems are analysed with regard to protective effectiveness and economical benefit. New solutions are developed to fill the gaps. Experiments and numerical analysis are used to obtain generalized results. Thus, a protection product portfolio is generated that assists to improve the most vulnerable components of critical infrastructure.

6 EU Regulatory Framework

Hitherto, normal regulations and building guidelines do not take into account the CBRE threat. So, based on the results of the project recommendations for new guidelines and standards for the design and retrofit of built infrastructure against terrorist CBRE threats will be formulated.

7 Integration tool development

One of the main aims of the SPIRIT project is to make the specialist knowledge available and easily accessible for the design and planning of the built infrastructure. A safety integrated design is needed in which also the vulnerability of a building, an asset, to CBRE threat is considered. To enable such an integrated design, a method to quantify the potential loss of functionality and structural integrity due to CBRE attacks is needed. Therefore the results of the individual SPIRIT work packages on the threat scenarios, the classification of the buildings, the consequence modelling and the counter measures will be integrated and combined in a guidance tool.

The basic idea behind the guidance tool is:

- a building, an asset is known and defined;
- the asset might be a target for a CBRE terrorist attack;
- the user wants to know how vulnerable the asset is to various CBRE threats;
- the user wants to know the possibilities and effectiveness of countermeasures;
- the user needs a tool to support the decision on the necessity and the kind of protective measures.

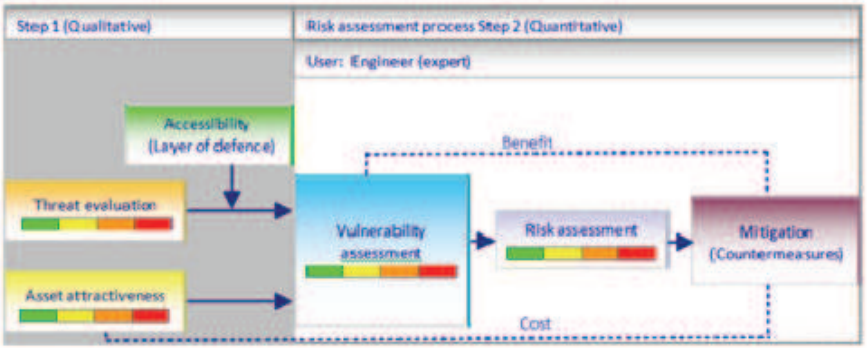

Figure 7.1: Concept of guidance tool

To answer all these questions quantitatively expert knowledge and classified information is needed. To meet the EU-requirements of public release, it was decided to make the guidance tool a two-step approach (Figure 3) [3], with a qualitative first step and a quantitative second step. Also the typical user for the two steps differs.

Step 1 is for the non-expert user to make a rough estimate of the asset vulnerability for threat scenarios covered by the SPIRIT project. Step 1 is qualitative and will be based on non-restricted information and uses no, or only very simple calculations. Basically, in this phase, the critical conditions for the asset, or modules of the asset, are identified. This SPIRIT Step 1 model will have a web-based format and the distribution is non-restricted.

In the second step, the initial vulnerability and the effectiveness of countermeasures are quantified. In this Step 2 restricted information may be used and the results are obtained by numerous calculations. This second part of the tool is intended to be used by experts only and the distribution will be restricted.

The tool provides guidance for the assessment in two parts (see Figure 3): 1) asset attractiveness, and 2) threat evaluation. The output is a ranking of the vulnerability of the asset to the various scenarios. Figure 7.2 shows as an illustration the asset attractiveness module, where the building is characterized through the input of several building and module characteristics.

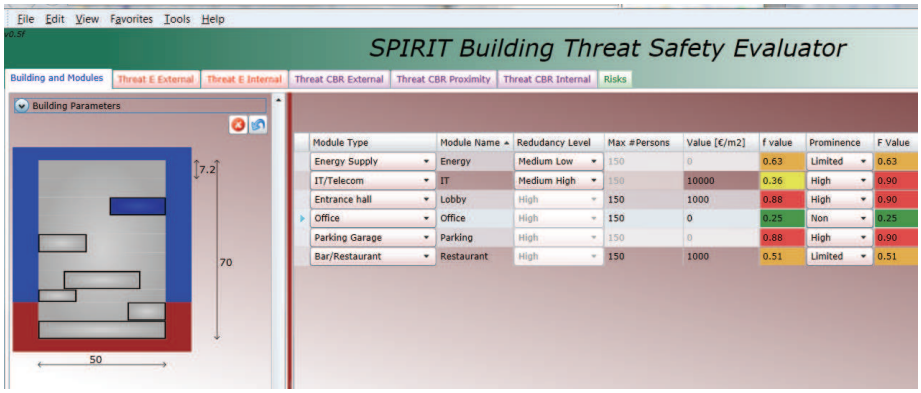

Figure 7.2: Guidance tool: asset attractiveness module (current version)

8 Concluding remarks

The SPIRIT project will provide the technology and know-how for the protection of buildings and people against terrorist threat and to minimize the consequences of a terrorist attack. The results presented in this paper are the first step towards this overall aim, with the guidance tool as the tangible result and the instrument for the knowledge transfer. The project progress can be followed on www.infrastructure-protection.eu.

References

[1] Veld, Frank van het; Groenli, Anders; Nöldgen, Markus: Selection of representative scenarios, SPIRIT D1.3, June 2011.

[2] Veld, Frank van het; Groenli, Anders: Database on CBRE incidents, SPIRIT D1.1, June 2011.

[3] Weerheijm, Jaap; Pronk, Sander; Progress report 1 on development of SPIRIT tool, Step 1; (DRAFT), June 2011.