PROTECTION AND RESILIENCY FOR SINGAPORE'S CRITICAL INFRASTRUCTURES

ONG Kwee Siang Steve, CHONG Oi Yin Karen, SEE Thong Hwee

ABSTRACT

The approach to designing critical infrastructure so that they are protected against discrete and well-defined threats is generally well understood. However, in the face of asymmetrical threats and vague terrorist intentions, such protective design approaches are of limited use. The increasing connectivity and complexities of modern society can compound the problem, thus causing unintended consequences. It is therefore necessary to rethink how critical infrastructures should be secured.

This article draws from DSTA's experience in designing critical infrastructures for the Ministry of Defence and the Singapore Armed Forces. It illustrates how protection and resiliency can be balanced to improve the survivability of critical infrastructures, taking into account system connectivity, vulnerabilities and the means to enhance recovery. Diagrams are provided to illustrate ways to integrate R&D and findings from international collaborations in Protective Technology into designing for resiliency. Examples of numerical simulations and explosive tests are also used to demonstrate the necessary vigour needed in testing assumptions, validating concepts and developing an implementable solution. This article emphasises that thorough and responsible protective technology work must be nested within realistic tests and relevant experience.

Keywords: protection and resiliency, critical infrastructures, connectivity, survivability, protective design

INTRODUCTION

After Singapore gained independence in 1965, it was necessary to build up local protective design capabilities quickly for the development of key installations, defence infrastructure and facilities. Early protective design methodologies were based on protection against well-prescribed threats. These building designs were standardised and often replicated for greater developmental efficiency. The building design philosophy was to first specify the design-basis threat – comprising the weapon and stand-off, and then to design the building based on specific protection criteria. These criteria were often related to specific building responses to weapons threats, with the assumption that all critical contents within the building would have similar damage thresholds.

While this design philosophy was adequate in the past, society has seen rapid changes, especially over the last three decades. Advances in technology have resulted in globalisation and increased connectivity that have also changed the threat space. These new realities call for a review of the way Singapore's critical infrastructures are protected.

THE RISE IN MODERN SYSTEMS COMPLEXITY

The advent of the computer sparked rapid advances in technology, enabling product research, development and prototyping within a virtual environment. This reduced developmental time and costs greatly. Coupled with the growth of the Internet, the development of wireless and broadband technologies catalysed the growth of information technology, expanding network access. This has resulted in higher demands for information exchange and data connectivity.

The need to compete globally further drove the development of interconnected infrastructure systems to meet productivity goals. Most systems today are designed to integrate as one network to deliver capabilities and have become more complex as a result. This interconnectedness also means that failure in one component can result in cascading failures in other systems clusters. New threats, such as cyber attacks, have also sprouted and grown. Against this backdrop, new realities that challenge the way critical infrastructures are traditionally protected have emerged. Where people, critical equipment and functions were once housed in discrete critical facilities, they are now housed in connected networks of facilities.

NEW REALITIES - CHANGING THREATS AND EVOLVING NETWORKS

What Was Designed in the Past May Not Be Relevant Today… Threats Have Changed and Often, What Counts are Networks of Things Rather Than Standalone Facilities

The threats that protective buildings and infrastructure were designed against in the past have changed. The early types of weapons comprised different categories of artillery and 'dumb' weapons that were air dropped. This method was inaccurate and had limited penetration capabilities and range. Modern weaponry now ranges from guided weapons that can be fired from longer distances, to mass saturation threats from rockets, artillery and missiles. Warhead technology has advanced with more powerful explosives as well as different kill mechanisms such as shaped charges, runway denial rounds, fragmentation rounds and thermobaric charges. Fuse technology has also progressed to facilitate the development of penetrating warheads. These weapons of enhanced capabilities can be developed faster, making it harder for protective infrastructures to keep up with commensurate protection levels without overwhelming costs and disruptions to operations. Adding to this ever-evolving and wide spectrum of modern weapon threats is the need for critical functions to operate in networks of buildings and infrastructure. This gives rise to the question of whether the traditional approach to protective design will become obsolete in the future.

Increasingly, It Is Worldwide Connectivity That Emboldens Adversaries

Beyond spurring military weapons technology developments, worldwide connectivity has increasingly emboldened terrorist activities, spinning off emergent threats. Terrorism has evolved over the years, from one where there was little connectivity and where knowledge in bomb making was confined to a few, to a highly connected environment where decentralised, non-hierarchal leaderships collaborate, tap and share knowledge online easily. Furthermore, such decentralised but connected terrorist networks have become harder to detect. Terrorist organisations have thus turned the threat of increased exposure due to the use of the Internet and telecommunications into opportunities to better themselves and their operations.

Unintended Consequences Can Arise From Ever-Evolving Threats

Threats and their effects have become more unpredictable. The resulting complex consequences may not be anticipated during the design phase. The September 11 attacks on the World Trade Centre (WTC) and the Pentagon in 2001 used civilian aircraft as a weapon. While the WTC twin towers were designed to withstand aircraft impact and did so initially, the eventual collapse of the towers arose from the large magnitude of aviation fuel fires that weakened the building structure. Thus, the design of infrastructure has to consider a wide range of potential threats.

The Range of Potential Targets Can Spike Dramatically

Traditionally, the focus has been on the protection of key installations and not on soft targets. The Bali bombings in 2002, as well as the JW Marriot and Ritz Carlton bombings in Jakarta in 2009, all showed that soft targets are attractive to terrorists. The mode of operation in the Bali bombings comprised multiple attacks with the first bomb occurring inside a night club, and subsequent car bombs outside to cause maximum death and injury to fleeing victims. The Jemaah Islamiyah arrests in Singapore further drove home the point of potential terrorist attacks on the home front, with soft target lists extending to include selected train stations. As one considers these recent terrorist incidents, the list of facilities to protect can spike dramatically, draining at unprecedented rates the already limited resources for defence and security.

Modern Built-up Environments are Prone to Adverse Collateral Damage Far Beyond the Immediate Vicinity of a Blast

Beyond connectivity enabled via computer networks, connectivity arising from the need to build and operate in dense clusters can make it difficult to anticipate where threats can emerge from, and which threats should protective design be applied to. Attacks against targets can result in collateral damage with widespread impact. The bomb attack in September 2004 on the Australian Embassy in Jakarta was one against a relatively hard target. It resulted in 11 fatalities in the immediate vicinity. While the embassy structure remained intact, windows in adjacent buildings up to 500m away shattered, injuring more people.

The direct and indirect effects of a blast detonating in a typical urban street are illustrated in Figure 1. The extent of injuries due to primary and secondary effects in this hypothetical scenario was assessed using DSTA's in-house consequence

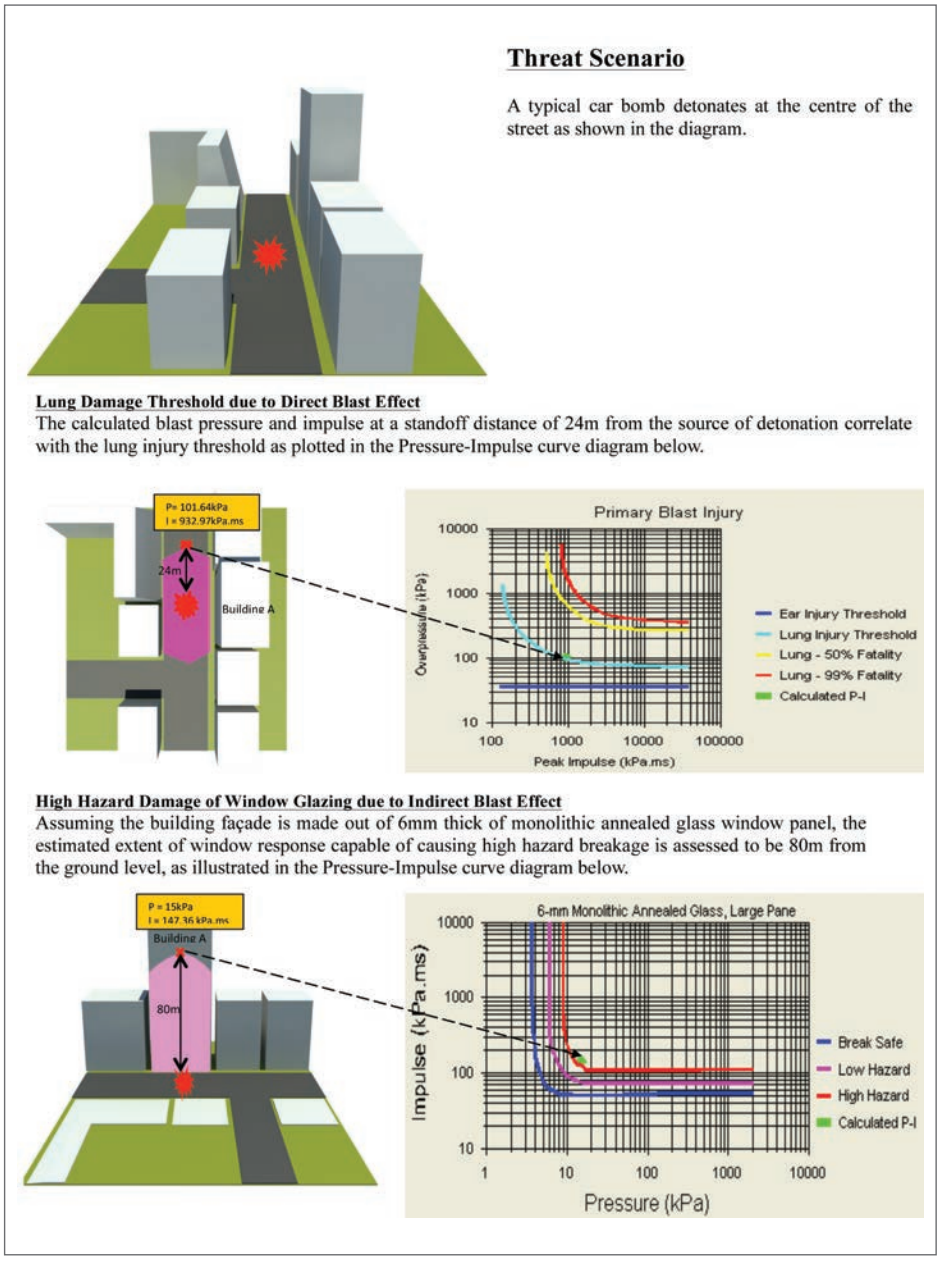


Figure 1. Hazard area under primary and secondary blast effects

analysis tool. From this illustration, it is evident that secondary effects of blast like glazing damage or debris hazards in a built-up environment resulted in human casualties in zones that extended far beyond the immediate vicinity of a blast.

The Diverse Spectrum of Operating Networks and Constituents Require Varying Tailored Protection

In the past, systems were less automated with low interconnectivity to operating networks beyond protected facilities. Today, relatively small incidents can have widespread impact in terms of connectivity and function. The fire incident at the Bukit Panjang Exchange on 9 October 2013 resulted in the breakdown of telecommunication services in the northern and western parts of Singapore. This affected telecommunications and broadcast services to 270,000 subscribers, including residential users, a few government agencies, financial institutions and businesses. A similar shutdown in critical communications systems such as air traffic control can result in potentially wider consequences.

Impact Often Extends Beyond Initial Design Boundaries

Key installations have traditionally been given standalone protection. However, the people operating these installations live as part of the wider community. The outbreak of Severe Acute Respiratory Syndrome (SARS) in 2003 has shown that threats such as pandemics can disrupt all sectors, ranging from air travel to health services. Likewise, when designing against threats like those from bombs, one has to look beyond the project boundaries to ensure that the placement of protected developments in an area does not 'pass on' threat effects to neighbouring areas.

Protective engineering is evolving from a unique auxiliary capability initially meant only for specialised facilities into a common feature for an infrastructure that takes into account the protection of the community that it is a part of. This demands not just a change in technology or analyses, but also a change in mindset to look beyond one's own task area.

To avoid being under-designed in protection against potential threats, radically different approaches to critical infrastructure protection are required.

NEW APPROACHES TO CRITICAL INFRASTRUCTURE PROTECTION

Infrastructures should not only be able to withstand attacks, but also recover after an attack and resume function. As such, it is necessary to build resiliency into critical infrastructures.

Resiliency is the ability to resume normal operations and function after an attack. Developing infrastructure resiliency does not only mean improving the physical protection of infrastructures to withstand attacks. It also allows the infrastructure system to sustain limited extent of damage, with recovery systems that have been put in place to ensure return to normalcy within a short time. A balance needs to be struck between providing full physical hardening and designing to allow partial damage with swift system recovery.

Designing a system with resiliency is a prerequisite for the continued survival of communities after attacks. Systems designed with resiliency have particular attributes which enable communities to recover quickly from disasters. These attributes include the ability to resist, absorb, recover from and adapt quickly to disruptions, and to resume system performance. Some level of system damage may be acceptable.

Resilient system design begins with an intimate understanding of how a system works as well as how it degrades and recovers. This, together with the ability to determine the exact levels of system damage sustained, allows components to be enhanced where the repair and system recovery can be done within required time frames.

Design for resiliency can be achieved through a right combination of protective engineering design, system redundancy, design robustness and contingency planning to counter asymmetrical threats or disruptions.

In the *Art of War*, ancient military strategist Sun Tzu, wrote: "知彼知己，百戰不殆". This is translated as "Know your enemy and know yourself, and a hundred battles can be fought without losing a single one". In the context of designing protective infrastructures, knowing your enemy involves understanding the threat. Knowing yourself involves understanding the operational needs and potential weaknesses.

The boundaries of this paradigm can be extended. Apart from knowing yourself and the enemy, understanding the interconnections with surrounding elements is just as important as it raises awareness of what could potentially go wrong.

These form the backbone of designing for resiliency with the preservation of an infrastructure's core capability in mind.

What Emerges From the Extended Paradigm

Protection Concept Development Without Definition of Threat

It is possible to design facilities for protection without defining a precise threat. This is done by expanding the area of coverage beyond the immediate facility, considering systems vulnerabilities and designing to incorporate mitigation systems. For example, a new annex building next to a cluster of key buildings may be constructed and the question of how resilient or protected should the annex be arises. The base level of protection and protective detailing can be determined by examining the annex building in relation to the existing cluster, and the effect of the cluster's surroundings in introducing threats to the annex building. After this, a detailed examination of the annex building's constituents can be carried out and specific areas further reinforced if necessary.

Beyond the design of buildings, the concept of developing protection options without a precise threat can also be applied to infrastructure networks, including networks for power and fuel. When an engineer designs a power or fuel distribution network system infrastructure, factors to consider include the type of critical function that the network supports and the environment the network is operating in, as opposed to waiting for the definition of the threat. As part of the design iterations, the network design can be scrutinised and vulnerabilities identified.

Vulnerabilities can include a single-point-of-failure, common modes failure and areas where even rudimentary forms of protection do not exist. Strategies to overcome single-points-of-failure in the system can include the incorporation of alternate distribution paths to critical nodes, or the physical separation of critical distribution nodes. Strategies to overcome common mode failures can include the use of independent backup. For fuel distribution networks, backup can come as alternate fuel supply from fuel bowsers. In the context of power distribution networks, this can be standalone backup generators.

Customised Protection of Critical System and Equipment

Considering the varying damage tolerance of different systems, physical hardening needs to be customised to match what the buildings contains. In the event that the threat is bigger or different from what was anticipated in the hardened design, or if the cost of hardening is prohibitive, other means to ensure system availability and quick recovery are needed. For example, there are several options to protect a satellite antenna dish against weapon effects. To minimise threat exposure, the mission critical system can be sited away from areas prone to attacks. To reduce time needed for recovery, mobile antennas can be utilised.

Future protected facilities need to move away from mass produced one-size-fits-all approaches to customised ones designed not just for the individual facility, but for a larger network or community which the facility is a part of.

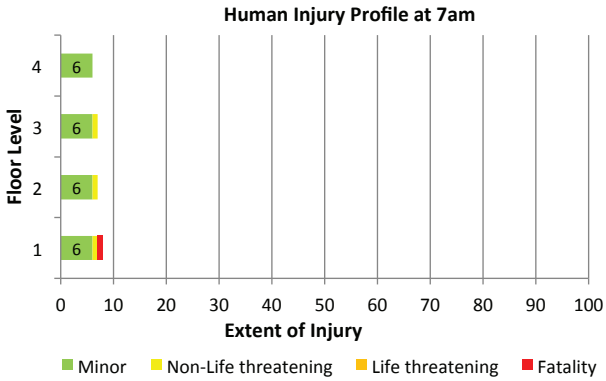
Including Time Domain and Usage Pattern Considerations When Designing Critical Infrastructure Protection

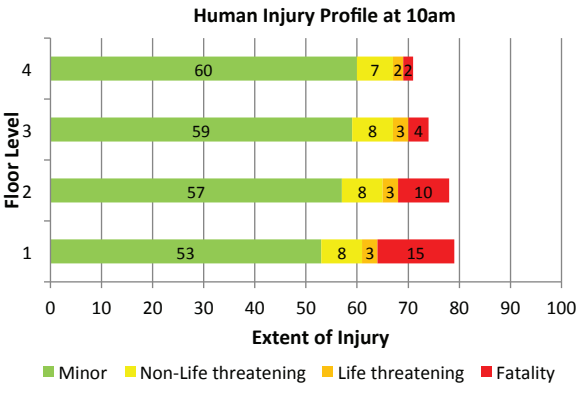
Improving resiliency through system design in space alone may not suffice. Operational characteristics such as time and usage patterns need to be considered. How people respond plays an important role in achieving mission success. Understanding how people respond to crises over time and how usage of infrastructures varies as stages of a crisis unfold will be essential. Building hardened shelters in public underground train stations may provide protection to masses of travelling commuters in times of crisis. However, people in high-rise residential buildings may not able to get to the public shelter in time. For them, individual household shelters meet their protection needs better because they can get to the shelters quickly and can carry on with other activities in between alerts. This allows a greater level of normalcy even in times of tension, with benefits for the population to be able to weather prolonged periods of tension in crises. Furthermore, a shelter serves multiple uses, including community use for public shelters and family use for household in peace time. However, one must not over optimise designs or try to squeeze too many usage patterns into a protected design. In the case of household shelters, if the shelter is used only as a storeroom it might not fulfil its original intent to shelter families without preparations to empty out massive stores.

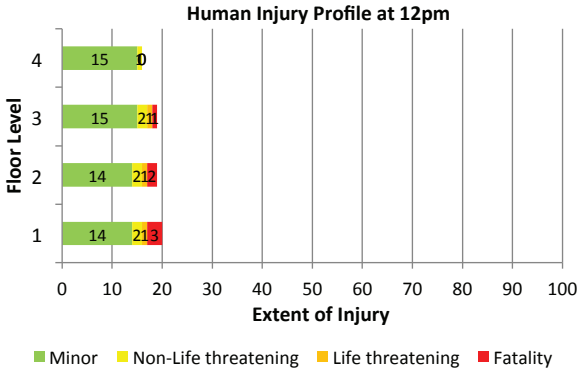
Checking Complex Usage Interactions in Time and Space for Emergent Vulnerabilities

The probability of threat occurrence and severity of its consequences can fluctuate over the time-space domain. Figure 2 illustrates the expected profile of human injury in an office building when a large bomb detonates at the front of the building over different times in the day. Changing the operational flow within the infrastructure facility can mitigate the effect. For example, the consequences of an explosion at an operational facility can be reduced by varying the times when people move through a building such that it does not coincide with times when a large bomb may be around. A thorough understanding of the operational processes over time is needed. Table-top exercises should be conducted to simulate operational processes and study how people and processes react to the introduction of disruptive events. This would also help planners and designers appreciate how infrastructure systems and people respond to crises. Realistic training regimes will further build up confidence and know-how in crisis management.

Beyond the focus on modelling weapons effects on buildings, modelling and simulation can be extended to workflow analysis, and can enable design optimisation for survivability and resiliency. For facilities where mass congregation of people or vehicles is expected during operation, modelling to simulate human and traffic flows will provide critical inputs to planners, designers and stakeholders on the adequacy of infrastructure system for mission support. Ground exercises are needed to validate planning and design assumptions. From this understanding, an estimate of how much and where protection and resiliency can best be injected into a building system can be made.







Threat Scenario
A large bomb detonates at standoff distance of 10m from the 5-storey office building outline as shown in the diagram.
Building Information
Height = 30m ; Offset = 25m; Width = 50m ; Span = 50m
Total Occupancy = 100pax per floor (total = 400pax in building)
Assumed Occupancy = 5%(7am); 100%(10am); 25%(12pm)

Figure 2. Expected human injury profile over different times of the day

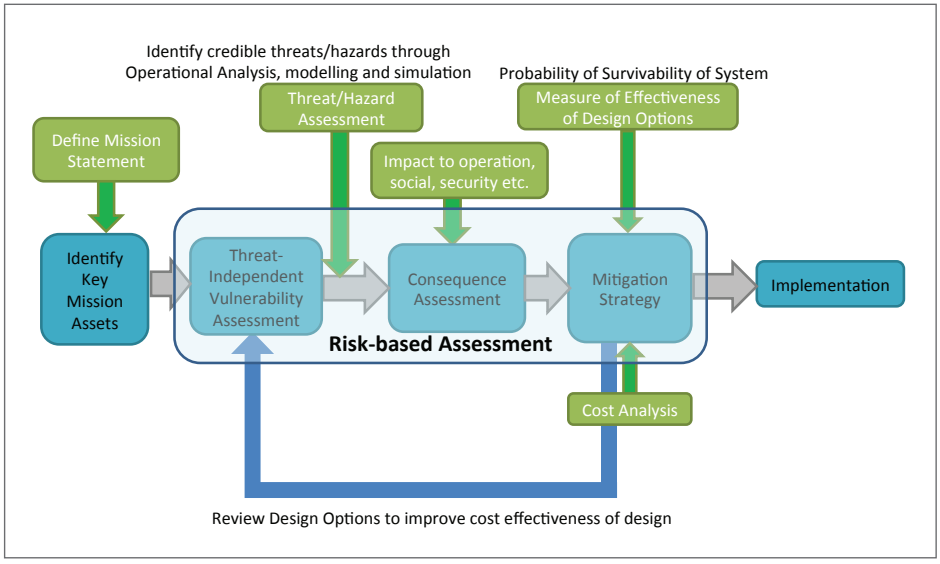


Figure 3. Vulnerability and consequences assessment framework

OPERATIONALISING THE NEW CRITICAL INFRASTRUCTURE PROTECTION DESIGN FRAMEWORK

A systematic and iterative approach to identify credible threats and address the comparative risks and vulnerabilities is illustrated in Figure 3.

Mission Identification and Vulnerability Assessment

The process of designing critical infrastructures begins with knowing the mission and identifying mission critical assets that need to be protected. A threat independent vulnerability assessment is then conducted to identify single points of failure, common modes failure, and areas of inadequate protection.

Consequence Assessment

Threats are then introduced and consequences to functionality and collateral effects are analysed. For a car bomb threat, parameters of interest include the location of the bomb in relation to the building. Consequence assessments are performed using physics-based computational models to derive blast loads on the building. These blast loads are then used to assess how the targeted building responds and the collateral effects on surrounding buildings. DSTA has conducted a large body of research work on explosion effects, structural response and progressive collapse in collaboration with local research institutes and overseas collaborators. DSTA has also built up computational know-how to model explosion effects. Explosive tests are conducted to ensure the validity of the research outcomes and models against realistic threats. Figure 4 illustrates a collaborative explosive testing effort to derive blast pressure data for validation against numerical blast prediction models.

Research outcomes are codified into analysis software and design guides that can be accessed by a wider pool of engineers. Figure 5 shows data from explosive tests conducted on local window types to ensure that the window performance is consistent with predictions from fast running tools.

Mitigation

Once potential consequences have been assessed, systems to mitigate vulnerabilities and consequences are developed. Operational analysis tools can be used to quantify the effectiveness of different design options, thereby facilitating design optimisation.

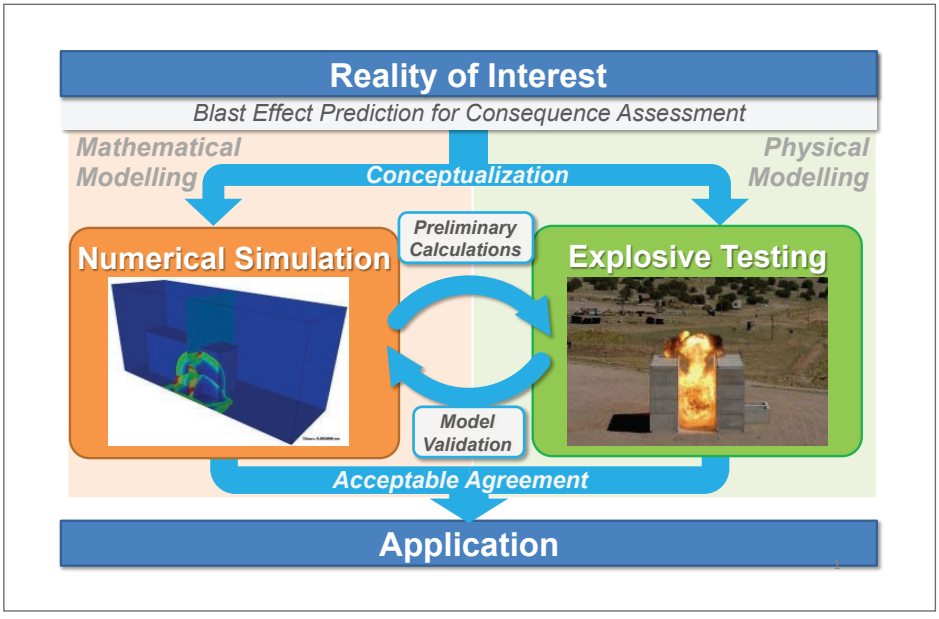
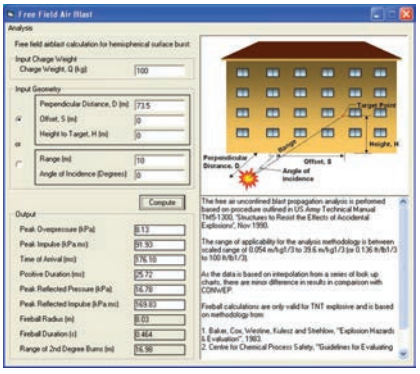
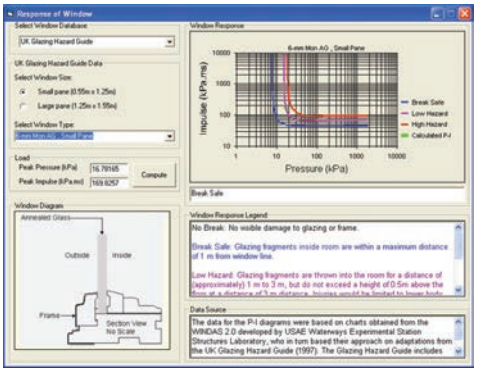


Figure 4. Validation of numerical models through collaboration with US Combating Terrorism Technical Support Office on urban canyon explosive tests

Observed damage in the low hazard range



Prediction of Blast Loads



Window Response Module

Figure 5. Comparison between window response explosive test results with in-house engineering tools for explosion consequence assessment

Optimising Resources to Yield Cost-Effective Solutions

To ensure resource optimisation, cost-benefit analysis is carried out on various implementable design options. The relevant stakeholders must strike a balance between the financial commitment to improve system resiliency and the acceptance of residual risk associated with time for attacks.

Closing Technology Gaps

DSTA is involved in research work to close technology gaps in critical infrastructure resiliency. These have evolved from the traditional focus on hardening infrastructures to resist and absorb extreme loads, to programmes that facilitate system resiliency and recovery. One such research programme derives data on the survivability of buried utility networks against weapons attack. The data is incorporated into an operational analysis tool that determines the overall system utility network survivability using fault tree analysis.

CONCLUSION

This paper illustrated how achieving a balance between protection and resiliency can improve the overall survivability of critical infrastructures. A critical infrastructure design framework was also discussed, which involves more effort spent assessing one's own vulnerabilities and interconnections than before. It is also coupled with greater efforts to look beyond traditional project boundaries constantly.

However, protection of critical infrastructure systems can lag behind technological advancements and resourcefulness of adversaries. Therefore, the design of critical infrastructures needs dogged perseverance and an attention to detail. Implemented protection concepts should be reviewed periodically, or run the risk of obsolescence. More often than not, lapses in protection of a critical infrastructure system surface only after attack events. The review of protective concepts needs to be carried out collectively by both technical and operational communities. Thereafter, the potential for future upgrades should be incorporated into the protective design where possible.

REFERENCES

Attack by Stratagem. (n.d.). In *Chinese Text Project*. Retrieved from http://ctext.org/art-of-war/attack-by-stratagem

Corley, G., Hamburger, R., & McAllister, T. (2002). Executive summary. In T. McAllister (Ed.), World Trade Center building *performance study: data collection, preliminary observations, and recommendations* (pp. 1-7). Retrieved from http://www.fema.gov/media-library-data/20130726-1512-20490-7075/403_execsum.pdf

Infocomm Development Authority of Singapore. (2014, May). *Fire Incident at Bukit Panjang Exchange on 9 October 2013*. Retrieved from https://www.ida.gov.sg/~/media/Files/About%20Us/Newsroom/Media%20Releases/2014/0506_CompletesInvestigation/Factsheet_FireIncidentBukitPanjang.pdf

National Consortium for the Study of Terrorism and Responses to Terrorism. (2004). Incident Summary. In *Global Terrorism* Database. Retrieved from http://www.start.umd.edu/gtd/search/IncidentSummary.aspx?gtdid=200409090001

BIOGRAPHY

ONG Kwee Siang Steve is a Manager (Building and Infrastructure) involved in the design development and project management of building infrastructures for the Ministry of Defence and the Singapore Armed Forces. He is also part of the multi-disciplinary DSTA team that carries out vulnerability assessments and mitigation studies. Steve graduated with a Bachelor of Engineering (Civil Engineering) degree with First Class Honours from Nanyang Technological University in 2006. He further obtained a Master of Science (Project Management) degree from the National University of Singapore (NUS) in 2013.

CHONG Oi Yin Karen is Head Engineering (Building and Infrastructure) who is driving R&D efforts in Protective Engineering. She has extensive experience in explosive testing, protective systems design and blast modelling and analysis. She won the Defence Technology Prize Team (Engineering) Award in 1999, 2006, 2007 and 2011. Karen graduated with a Bachelor of Science (Nuclear Engineering) degree with First Class Honours from Queen Mary College, University of London, UK, in 1986. She further obtained a Doctor of Philosophy (Nuclear Engineering) degree from Queen Mary and Westfield College, University of London, UK, in 1991.

SEE Thong Hwee is Head Capability Development (Building and Infrastructure) who oversees building infrastructure development of joint facilities. He also provides protective engineering consultancy for critical infrastructures. Thong Hwee has played a key role in extending DSTA's protective technology capabilities to Singapore's homeland security. He was involved in numerous projects that improved the physical resiliency of critical national infrastructures, such as the national power grid, mass rapid transport network, various government facilities and several iconic building developments. Thong Hwee graduated with a Bachelor of Engineering (Civil Engineering) degree with Honours from NUS in 1997. He further obtained a Master of Science (Engineering Mechanics) with Specialisation in Explosives Engineering, from the New Mexico Institute of Mining and Technology, USA, in 2002.

NOTES

NOTES