Argonne
NATIONAL LABORATORY

The Journal of Physical Security

Volume 4(2), 2010

THIS ISSUE...

JPS

Table of Contents
Journal of Physical Security, Volume 4(2), 2010
ISSN 2157-8443
Web: http://jps.anl.gov

Editor's Comments

Welcome to the second issue of volume 4 of the Journal of Physical Security (JPS). This is the first time that we have published two issues in the same year. This issue contains papers about securing houses of worship, estimating explosive blast damage, the differences between threats and vulnerabilities, and emerging new security paradigms.

As usual, the views expressed in the Journal of Physical Security are those of the respective authors and should not necessarily be ascribed to Argonne National Laboratory or the United States Department of Energy.

There continues to be considerable enthusiasm for JPS on the part of the readership, but also a lot of trepidation among potential authors who are considering submitting manuscripts. (I know this because they often call me up with potential topics, worried about proceeding.) Authors who have published in JPS have found the process rewarding, have gained fresh insight into important security issues, and have educated a lot of readers on important security points. Please consider submitting a manuscript and encouraging colleagues and students to do likewise!

What follows are some rambling thoughts about physical security vs. cyber security, the importance of a stiff upper lip, patents and security, and how to spot Security Theater.

I gave the Keynote Address at the 19th Annual USENIX Conference in Washington, D.C. in August. (See http://www.youtube.com/watch?v=51MxGK2q7Wo) This was the first time I've attended USENIX. I was very favorably impressed with the quality of the presentations and the work they represent. I was also struck by how different the cyber security culture is from the physical security culture.

This difference greatly complicates the Convergence problem—also known as the "Thugs vs. Nerds" problem—which is the bringing together of physical and cyber security. Increasingly, good cyber security requires better physical security, and physical security practitioners find themselves working with software programs and with hardware devices that are interfaced to complex cyber networks and/or have substantial embedded computing or microprocessor power. Cyber vulnerabilities can quickly become physical security vulnerabilities, and vice versa.

Having moved around a bit in both worlds, here are my lists of what cyber security professionals and physical security professionals can potentially learn from each other:

What Physical Security Professionals Could Learn from Cyber Security Professionals

- Vulnerabilities are numerous, ubiquitous, inevitable, & constantly evolving.
- They don't automatically mean somebody has been screwing up.
- Scapegoating isn't very helpful.
- Security is not binary, it's a continuum.
- Customer focus: productivity has to be an issue in security.
- How to motivate good security practice among regular employees.
- Past criminals can make good consultants.
- Technology is not a panacea—security is really about people.
- Regular employees *are* the security, not the enemy of security.
- Lose the coat & tie!

What Cyber Security Professionals Could Learn from Physical Security Professionals

- Discipline, Leadership, Organizational Skills, & Being a Team Player.
- Understanding where you fit into the organization.
- Techniques for dealing with upper management; Making the business case for security.
- Effective project management & budgeting; meeting deadlines.
- Females can be very effective security professionals.
- Street smarts, people skills, & a good understanding of psychology.
- Dealing with Social Engineering & the Insider Threat.
- Realization that good cyber security requires good physical security.
- Maybe that T-shirt could be washed once in a while!

A recent article in the *Financial Times* (Page 17, September 5/5, 2010) got me thinking about 9/11. The article claims that, "Even at the height of the Blitz, Londoners were more bothered by the weather."

Most of the victims of the German bombing of England (the "Blitz") in World War II were civilians. A total of 43,683 people were killed by the Blitz in London alone by May of 1941. Many Londoners took shelter at night, including in the Underground.

Despite the bombings and the disruption to daily life they caused, a December 1940 survey of Londoners asked them to rank what most impacted their lives and their feelings. They ranked the "weather" first, "general war news" second, and "air raids" only third. This is surely an example of great courage and the famous British "stiff upper lip".

By comparison, the loss of 2,752 lives in New York on 9/11 due to murderous terrorists—as horrific as it was—involved much less loss of life. In fact, the following table lists various causes American deaths in 2001, most of which were preventable.

2001 Causes of American Deaths	Number
9/11 Terrorism	2,752
Drunk Driving	17,448
Not Wearing Seat Belts	19,146
Guns	29,573
Deaths Due to Smoking	428,000

The next table lists the approximate lifetime odds of an American dying of various causes. It shows that terrorism is not a very high risk factor.

Cause of Death	Lifetime Odds
Cancer	1 in 5
Automobile Crash	1 in 83
Suicide	1 in 119
Murder (not due to terrorism)	1 in 210
Walking Across the Street	1 in 625
Airplane Crash	1 in 5,000
Lightning	1 in 80,000
Terrorism	1 in 88,000

So, while it is true that (1) the cowardly and murderous acts of 9/11 are unacceptable, (2) they resulted in a terrible loss to the victims' families, (3) the animals responsible need to be hunted down, and (4) we need as effective a level of homeland security as is prudent, the obvious question is why did 9/11 change America? Terrorists win—even when nobody dies—when they generate fear, cause us to modify our lifestyle, and/or make us compromise our basic values and principles for an illusionary goal of absolute safety. Perhaps we could use more of the Brits' stiff upper lip.

I'm always amazed when manufacturers of security devices and systems tout the fact that their product is patented as if this was a good thing. By law, patents have to be fully enabling. Thus, while it may be entirely proper and prudent for a manufacturer to patent inventions, a patent is not a positive security attribute, it is a vulnerability. It explains (including to the bad guys and vulnerability assessors) how everything works.

Bruce Schneier coined the term "Security Theater" to describe the situation where phony security measures provide a feeling of improved security, but in reality provide little or no actual security. Another name for Security Theater is "Ceremonial Security".

As a vulnerability assessor, I frequently find Security Theater across a wide range of different physical security devices, systems, and programs, as well as in domestic and international nuclear safeguards. It's important to realize, however, that Security Theater is not automatically a bad thing. It can present the appearance (false though it may be) of a hardened target to potential adversaries, thus potentially discouraging an attack (at least for a while). Security Theater can reassure the public while more effective measures are under development, and help encourage employees and the public to take security seriously.

In international treaty monitoring and verification, Security Theater can help foster an environment of transparency, trust, confidence-building, and international cooperation. Security Theater can provide great photo opportunities for national leaders trying to promote disarmament regimes that may face intense political opposition. It can also serve as a first step in creating new regimes (because Security Theater is always easier than real security). During treaty negotiations, Security Theater can serve as an easy-to-negotiate stand-in for more rigorous security and safeguards procedures to be developed and negotiated in the future. Perhaps most importantly, Security Theater can provide an excuse to get inspectors inside nuclear facilities where their informal observations and interactions with host facility personnel can be of great value to disarmament, nonproliferation, and safeguards efforts.

The real problem occurs when Security Theater is not recognized as such, or when it stands in the way of good security or is actually preferred over real security (because it is easier).

The best way to spot Security Theater is to critically analyze the security it purports to offer. This, however, takes a lot of work. An easier way is to look for the attributes commonly found with Security Theater. The following is my list. If a third or more of these attributes reasonably apply to a given security device, system, measure, or program, it is likely to be Security Theater. The more the attributes apply, and the more of them that apply, the more likely you are looking at Security Theater, not real Security. (For more information, see RG Johnston and JS Warner, "Security Theater in Future Arms Control Regimes", *Proceedings of the 51st INMM Meeting*, Baltimore, MD, July 11-15, 2010.)

<u>The Security Theater Attributes Model</u>: The following are the typical attributes of technologies, measures, and procedures that are Security Theater. They are listed in no particular order.

1. There is great urgency to get something out in the field, or at least its acceptance negotiated.

2. The promoters and developers of the technology or procedure earnestly—even desperately—want it to solve the security or verification problems. (Strong proponents of nuclear disarmament and nonproliferation efforts often intensely wish, quite admirably, to make the world safe from nuclear hazards. This can sometimes lead to wishful thinking.)

3. There is considerable enthusiasm for, great pride in, and strong emotion behind the proposed (or fielded) technology or procedure.

4. The technology or procedure is a pet technology of the promoters and developers, not necessarily the technology or procedure that was chosen from among many candidates as a result of a careful study of the specific security/safeguards/verification problem of interest.

5. The security/safeguards/verification technology or procedure is viewed with great confidence, arrogance, and/or represented as “impossible defeat” or nearly so. (Effective security is very difficult to achieve. Generally, if promoters and developers of a given security or safeguards approach or hardware have carefully considered the real-world security issues, they will not be in such a boosterism mode. Fear is, in fact, a good indicator of a realistic mindset when it comes to security.)

6. There is a great deal of bureaucratic or political inertia behind the technology or procedure.

7. Substantial time, funding, and political capital has already been spent developing, promoting, or analyzing the technology or procedure.

8. The people or organization promoting the technology or procedure have a conflict of interest, or at least are unable to objectively evaluate it.

9. No vulnerability assessors, people with a “hacking” mentality, devil’s advocates, or creative question-askers have closely examined the technology or procedure (perhaps because they weren’t allowed to).

10. Anybody questioning the efficacy of the technology or procedure is ignored, attacked, ostracized, or retaliated against.

11. The people developing or promoting the technology or procedure have no real-world security experience.

12. The people developing or promoting the technology or procedure are mostly engineers. (No insult to engineers intended here. In our experience, the mindset and practices that makes one good at engineering aren’t the optimal mindset for good security. Engineers tend to work in solution space, not problem space. They tend to view Nature and stochastic failures as the adversary, not maliciously evil people who attack intelligently and surreptitiously. They strive to design devices, hardware, and software that are user friendly, easy to service, and full of optional features—which tends to make attacks easier.)

13. Vulnerabilities are only considered, and vulnerability assessors only involved, after the development of the technology or procedure has been nearly completed. (At this point, it is usually too difficult to make necessary changes to improve the security for economic, political, timeliness, or psychological reasons).

14. The technology or procedure involves new technology piled on existing technology or

procedures in hopes of getting better security, but without actually addressing the Achilles heel of the old technology or procedure.

15. The technology or procedure relies primarily on complexity, advanced technology, the latest technological “fad”, and/or multiple layers. (High technology does not equal high security, and layered security isn’t always better.)

16. Any consideration of security issues focuses mostly on software or firmware attacks, not on physical security.

17. The main tamper detection mechanism—if there even is one—is a mechanical tamper switch or an adhesive label seal. (This is approximately the same, in our experience, as having no tamper detection at all.)

18. The technology or procedure is not directed against a specific, well-defined adversary with well-defined resources.

19. The end users of the technology or procedure have never been consulted and/or the technology or procedure is being forced on them from above. (These are people who understand the real-world implementation issues, and are the ones who will have to make the technology or procedure actually work).

20. The technology or procedure is not well understood by the non-technical people proposing or promoting it (or by the people in the field who are to use it), and/or the terminology being used is misleading, confusing, or ambiguous.

21. Particularly with security procedures: control or formalism gets confused with security.

22. Domestic and international nuclear safeguards get confused. (These two security applications are remarkably dissimilar.)

23. The technology or procedure in question makes people feel good. (In general, real security doesn’t make people feel better, it makes them feel worse. This is because it is almost always more expensive, time-consuming, and painful than Security Theater. When security or safeguards are thoroughly thought-through, the difficulty of the task and knowledge of the unmitigated vulnerabilities will cause alarm. Fear is a good vaccine against both arrogance and ignorance.
This is the basis of what we call the “Be Afraid, Be Very Afraid Maxim”: If you’re not running scared, you have bad security or a bad security product.)

24. The use protocols for the technology or procedures are non-existent, vague, or ill-conceived.

25. The security application is exceeding difficult, and total security may not even be possible.

26. The terminology is vague, confusing, misleading, or full of wishful thinking, e.g., “high security”, “tamper-proof”, “pick proof”, “undefeatable”, “due diligence”, “barrier”, “certified”,

“fully tested”, “reliable”, “real-time”, “zero error rate”, “unique”, “industry leader”, “industry standard”, etc.

-- Roger Johnston, Argonne National Laboratory, September 2010

Security Challenges for Houses of Worship

Brian M. Harrell, CPP
North American Electric Reliability Corporation (NERC)
Brian.Harrell@nerc.net

Abstract
Violence in American Churches is on the rise; churches today are no longer safe havens from the violence of their communities and religious leaders face the unique challenge of providing an inviting and loving environment in the church without being mistaken for an easy target. Churches can no longer afford to ignore their security. The challenge for worship staff is preventing the potential victimization of worship members and visitors while asserting ones self as a "hard target" and maintaining the peaceful and welcoming milieu one expects at a house of worship. Unfortunately, the religious community is subject to many of the same hazards that secular organizations face. These include both external and internal threats which can come in the form of street criminals, white collar criminals, hate groups, terrorists, ideology groups, and others. Typically, congregations are not prepared at all or at best are prepared minimally for the risks these groups present. This paper addresses the specific security concern and suggests a simple plan for action.

Key Words
Church security, active shooter, crime prevention, preparedness, religious attack

On Sunday, May 21, 2006, a gunman walked into a church in Baton Rouge, Louisiana, near the end of Sunday morning services. He proceeded to shoot five people at the church before abducting his estranged wife and three children. While the children were eventually released, the woman (wife) was later found dead at another location. The church's pastor was shot during the incident. Shocking as it may seem, violent incidents of this nature happen several times each year at churches across the country. Because places of worship are open to the public and often times inviting, churches have become more vulnerable to these senseless acts of violence.

American houses of worship are rarely the focus of security or crime prevention efforts. However, a 2009 report published by the Christian Security Network outlines 1,237 crimes against Christian churches including 12 homicides, 38 other violent incidents including, 3 sexual assaults, 3 kidnappings, 98 arsons, and over 700 burglaries resulting in more than $24 million in property loss (Hawkins, 2010). Faith leaders typically are not aware of vulnerabilities and basic crime prevention methods. Consequently, many churches, temples, synagogues, and mosques are soft targets. With over 600,000 ministers and over 400,000 Christian churches reported in America and a growing concern over church safety and security, faith and worship leaders are looking for opportunities to ensure they are providing a true safe environment for all their members. Faith-Based Organizations (FBO) have traditionally lacked the security measures and emergency preparedness planning that businesses and other secular groups have put into place. Indeed, many of these organizations are reluctant to discuss whether or not they are aware of ever having been targeted and what, if any, active security preparations they have put in place. Loss prevention typically has been discussed; however efforts at houses of worship are typically targeted toward internal losses and property crime. Preventing cash mishandling and property vandalism pose frequent challenges for worship facilities and this should not be underscored. If external threats could be controlled through effective countermeasures, the internal environment of houses of worship would benefit from a renewed interest in security methods. Consequently, much like shopping malls and other retail establishments, worship facilities do not offer the protection afforded by places with rigorous security screening procedures, such as airports or government offices.

Today we see a renewed interest in worship facility arson throughout the United States. Recent headlines reveal that active shooters have made their way into the front doors of our most sacred institutions, killing or maiming innocent individuals. Probably the most ominous potential threat is that of terrorists using primitive weapon systems, such as explosives acquired on the open market, to cause mass damage.

How does a faith-based organization deal with violent or destructive threats? How does proactive preparedness and basic security mesh with faith based organizations? For example: Most world religions are taught to prefer their brother/sister, to turn the other cheek, and to forgive and forget. This ideology can still exist while faith leaders “protect the flock”. While no worship facility is expected to hold off armed gunman by taking a military style defensive position, it can be reasonably expected for a house of worship to have evacuation plans, emergency contacts, and a security awareness posture (mind set) put in place. While worship facilities are doctrinally places of refuge and peace and all should be welcome, some basic behavioral detection techniques may identify a violent episode before it happens. Unfortunately, there are many examples of where violence took parishioners by surprise.

In October 2006, a man sloshed fuel on pews and parishioners during a church service and started a fire intended to kill everyone in the building. Two women were burned when their clothing caught fire. Fortunately for church members, staff was able to subdue the suspect while law enforcement responded. The police report later stated that the suspect admitted that he took gas cans and a knife to the Peoples Church in Salem Oregon with the intent of killing all the people in the church. Trial testimony indicated he thought he was acting on God’s orders. Mental health experts testified he had paranoid schizophrenia (Koe, 2006).

In 2007 a black-clad gunman walked into New Life Church, in Colorado Springs, CO on a typical Sunday and started shooting. Fortunately, he was met with the church's first line of defense: a congregant with a concealed-weapons permit and a law enforcement background (Gorski, 2007). The armed volunteer shot the gunman. New Life's pastor credited the church attendee with saving dozens more lives due to quick action.

The use of explosive devices is not just a foreign phenomenon any more, harkening back to the Irish Republican Army (IRA) bombing incidents in Great Britain. In Louisiana, four men allegedly broke the windows of Cypress Creek Baptist Church in Vernon Parish in July 2009 to steal electronic equipment. After that, the men are reported to have robbed a fireworks stand. Using the stolen explosive materials, they made three bombs. One was set off on a roadway in Vernon Parish, one was set off outside of the Champions Center at Grace Church, and one was left, but not detonated, in Three Pines Apostolic Church (Bulger, 2009).

In December of 1986 in Long Beach, CA the Morningland Church was the victim of a strategic bomb attack. A lone suspect was disturbed at the churches teachings and the “harassment” of a sister. The suspect smartly placed the concealed bomb within the church structure and subsequently, part of a 10-stick dynamite bomb went off. Thomas T. McCoy, 26 was arrested on suspicion of ignition of a destructive device, possession of a destructive device, and carrying a concealed weapon (Ex-Morninglanders, 2010).

While houses of worship typically have medical guidelines to turn to if someone has a heart attack or an evacuation procedure if there is a fire, not many would quickly know what to do if a person with a gun walked into the church, temple or synagogue. Unfortunately, the religious community is subject to many of the same hazards that any other organization faces. These include both external and internal threats which can come in the form of street criminals, hate groups, terrorists, white collar criminals, common criminals and others. Churches want to present an open and welcoming image, but in an era of mass-casualty shootings and terrorism threats, the above mentioned incidents highlight what should be a new emphasis on security. Some of the nation's estimated 1,200 megachurches — places where more than 2,000 worshippers gather each week — have been quietly beefing up security in recent years, even using armed guards to protect the faithful. Even without a security department, faith leaders can train volunteers to keep watch for suspicious behavior, such as a visitor dressed in a long coat during the summer or not making eye contact with fellow congregants.

Security professionals must understand that the faith-based community is different in many ways from the business or government setting. Because of the challenges identified above, emphasis should be placed on the application of:

- Crime Prevention Through Environmental Design (manipulating the built environment such as landscape designs, natural surveillance, and using structures to divert or influence flow);
- Physical security monitoring (alarms, cameras, access control);
- Security/terrorism awareness training for faith leaders;
- Establishing a security committee that produces preparedness plans; and
- Fostering positive relationships with local law enforcement

Balancing these considerations requires faith leaders to take a deliberate response to security. On one hand, embracing a fortress mentality with heavily armed guards and requiring all congregants to pass through metal detectors would hurt the faith's philosophy and be a monumental response to a low frequency event. On the other hand, going about business as usual without addressing security concerns would undoubtedly fall below the expectations of the congregation members you are serving.

So how should a worship facility and its staff prepare and respond to a future security threat? The first step in addressing security is to form security committee dedicated to studying the topic and ultimately, recommend options for the facility. If your congregation has a safety and security team currently in place, conduct a threat and vulnerability assessment for the property. You may want to obtain input from additional congregation members who have specialized experience in the field, such as those with backgrounds in law enforcement, the security industry, the military or emergency management (Spacek, 2008).

Once the threat and vulnerability assessment has been completed, the next step for the committee is to put together a draft security plan for the leadership's consideration. Local law enforcement agencies should be consulted as they will provide feedback and intelligence to which faith organization would not otherwise be privy to. Houses of worship should implement a layered security approach utilizing a defense in depth mentality. For example, parking lots offer the opportunity to suggest that the facility is a "hard target". The lot should be well lit, appropriately marked, and offer protection to foot traffic. Next, multiple layers of greeters or volunteers (outside, foyer-level, and sanctuary-level). Ideally, each layer of security should be able to communicate to the other. The goal is to identify threats early and respond as soon as possible. Combine a well trained staff with security enhancements such as cameras and physical locks, and this could be the difference between life and death. Other considerations in the plan may include:

- The roles and responsibilities of various layers of personnel
- Dealing with disruptive or impaired individuals
- Dealing with violent persons with or without a weapon
- Pastoral protection
- Lockdown and/or evacuation procedures
- Equipment needs
- Communication to each other and the congregation

One option a faith based organization has is to hire off-duty active law enforcement officers. An advantage in hiring these individuals is that they will have superior training and experience. However, the faith facility must still train these individuals in what their role will be in emergency situations. A contract security guard service is another option. With this decision, the facility still must undertake reasonable precautions in hiring the security service, such as checking references and fully understanding the service's screening, training, and supervision procedures.

Faith leaders should not simply accept the risk but rather seriously consider the consequences of having no plan at all, and as a response, instill the need to prepare an overall security strategy. A wide variety of resources are available to both security professionals and religious leaders.

The U.S. Department of Justice offers no-cost technical assistance to groups involved in projects to protect houses of worship. The process of seeking such assistance is explained in a publication titled *Church Arson Prevention Training and Technical Assistance Program*. The Justice Department will solicit information about the churches specific security need. If assistance is approved, the U.S. Department of Justice will contract the work to a private firm that will coordinate the assistance and search for a specialist whose expertise most closely matches the needs of the recipient. The recipient can also suggest a specialist and play a role in negotiating the type of assistance needed. Technical assistance, training, and evaluation are three primary forms of assistance that will enhance projects to protect houses of worship (DOJ, 1997).

The US Department of Homeland Security (DHS) provides a no-cost training presentation targeted at churches, temples, synagogues, masques and other places of worship. This training, titled *Soft Target Awareness Course (STAC)*, strives to bring awareness to faith leaders by education (highlighting the risk) and targeted awareness of anti-terrorism directives (DHS, 2010). In addition, this presentation advises about the effectiveness of signs, lighting, guards, perimeter security, and surveillance detection.

It is essential that those charged with leadership balance having a security presence while still keeping a house of worship open to everyone. One key component of a faith organizations security program is observant volunteers. These frontline roles are often the first people to see or hear problems, and often have access to all parts of the building before, during and after the service. But sadly, many greeters and ushers receive little or no training related to the role they can play in observing, getting help quickly, and providing leadership in an emergency situation (Rowe, 2009). Today domestic terrorism is often overlooked due to Middle Eastern events being displayed prominently in the media. However, when domestic terrorists or lone-wolfs are looking for an easy target with unsuspecting prey, they typically need not look further than their local neighborhood house of worship. Construct a security plan, plan for the inevitable, and be prepared!

About the Author

Brian M. Harrell, CPP is currently the Manager of Critical Infrastructure Protection for the North American Electric Reliability Corporation (NERC) which monitors the reliability of the Bulk Electric System (electric grid). Brian has spent his career consulting on antiterrorism, physical security, and infrastructure protection.

References

Bulger, L. (2009). Church bomb suspects face minimum seven years in prison. *Beauregard Daily News.* July 9, 2009.

Hawkins, J.A. (2010). *Crimes against Christian organizations in the United States.* Christian Security Network. Cincinnati, OH.

Ex-Morninglanders. (2010). *1986-Dec.: Morningland church bomb scare.* Retrieved March 28, 2010 from http://ex-morninglanders.com/news/news8.htm

Gorski, E. (2007). Armed guards now the norm for some U.S. megachurches. *The San Diego Union-Tribune.* December 11, 2007.

Koe, R. (2006). *Why did convicted killer target Salem church in fire? Pastor, others puzzled.* Christian News North West.

Purpura, P.P. (1999). *Securing houses of worship: A community services manual for ASIS chapters.* Alexandria, VA; ASIS International Press

Rowe, T.L. (2009). *Church security: How to access the safety and security of your place of worship.* Retrieved March 28, 2010 from http://tinalewisrowe.com/category/safety-and-security/the-greeter-and-usher-role/

Spacek, E. (2008). Prepare your church for the worst-case scenario. *Church Executive, vol. 2008,* 3.

US Department of Homeland Security. (2010). *Bombing prevention training.* Retrieved March 25, 2010 from www.dhs.gov/files/programs/gc_1265223119415.shtm

US Department of Justice. (1997). *Church arson prevention training and technical assistance program.* Retrieved March 28, 2010 from http://www.ncjrs.gov/pdffiles/fs000174.pdf

Probabilistic Estimates of Vulnerability to Explosive Overpressures and Impulses

David B. Chang (dbcsfc@aol.com)
Consultant
Tustin, California

Carl S. Young (carlsyoung@verizon.net)
Stroz Friedberg LLC
4th Floor, 32 Avenue of the Americas
New York, NY 10013

Abstract

A probabilistic risk assessment procedure is followed to estimate the probability of protection at facilities from vehicle-borne explosions. Using truncated normal distributions for both the TNT equivalencies of the charge and the standoff distances, a probability for protection is calculated for a single degree of freedom (SDOF) blast protection design curve. Numerical examples are given for two representative design curves that give probabilities of protection of 80% and 91%.

1. Introduction

Different scenarios can be envisioned that would be relevant to the design of terrorist mitigation measures at a facility. For explosive threats, one could assume a scenario in which the standoff distance is the minimum possible distance to the intended target, produces collateral damage to nearby facilities and that the explosive source is very large. For example, one such scenario might be 40,000 lb of an efficiently exploded ammonium nitrate/fuel oil mixture contained within an 18-wheeler. A related scenario might be where the 18-wheeler is located as close as physically possible to the intended target or where the size of the explosive source is not as large. If a smaller vehicle is envisioned to transport the source, 40,000 lb would be an overestimate of the explosive payload. In addition, the TNT-equivalent mass of the explosive can vary depending on the physical and chemical details of the explosive mixture.

The uncertainties in explosive strength and standoff distance suggest that a statistical assessment of the threat parameters could play a role in the mitigation design. This type of approach has been proffered recently by Stewart, Netherton, and Rosowsky (2006). In this reference they argue that there is so much uncertainty associated with terrorism that an attempt should be made to quantify the uncertainties, and that these results should then be used in established probabilistic risk assessment procedures to systematically assess the viability and relative benefits of different mitigation measures.

Netherton and Stewart (2009) considered the variability in explosive blast loading caused by a multiplicity of factors with respect to façade glazing, and used Monte Carlo simulation to calculate probabilities of glazing damage and safety hazards conditional on scenario-driven parameters.

The present paper also provides a statistical assessment of an explosive-borne threat to window structures in facilities. However, we adopt an exclusively analytic approach based on published scaling relations for the key explosive parameters, impulse and overpressure, as well as the design specifications of the window. Although it does not take into consideration every physical parameter that affects explosive impact (most notably the presence of intervening structures), this method obviates the need for computer simulation and yields a simple if approximate method to assess explosive risk.

Specifically, we estimate the probability of protection one might expect against likely blast overpressures and impulses. This is based on both the probability function for explosive strength and standoff distance and the design curve used for constructing components of a curtain wall façade, a popular form of construction for modern office facilities. In this paper, the design curve is derived from a simple single degree of freedom (SDOF) component model.

In addition, the method of assessing the probability of protection afforded by a specific building component as described herein can be generalized and applied to other security scenarios for which scaling relations exist for relevant physical parameters. This offers a potentially powerful tool in quantitatively assessing risk for a variety of scenarios.

Section 2 describes the probability distributions to be assumed for the TNT equivalence strength of the explosive source, and for the standoff distance between the explosive source and a potential target.

Section 3 discusses the blast parameters (overpressure and impulse) that determine the damage experienced by a structure.

Section 4 summarizes scaling laws that relate the blast overpressure and impulse to the explosive strength and standoff distance.

Section 5 then discusses a blast protection design curve that is based on a SDOF model and on data provided by a consulting firm for a specific window design.

Section 6 derives a specific blast mitigation probability of protection using the probability function and the design curve.

Section 7 discusses the specific results and generalizes the approach to other operational risk problems.

2. Probability distributions for explosive source strength and for standoff distance

Based on past terrorist explosive attacks on structures, we shall assume that the explosive source is an ammonium nitrate/fuel oil (ANFO) mixture, and that this explosive mixture is delivered to the near vicinity of a facility by a vehicle. Uncertainties exist as to both the TNT equivalency of the ANFO, and to how close the vehicle will be to a facility when the mixture is detonated.

2a. Uncertainty in TNT equivalency factor

The construction and the efficacy of the resulting bomb have been widely discussed in the open literature. Two readily available on-line summary articles are:

> Explosives – ANFO *Ammonium nitrate-fuel oil), at http://www.globalsecurity.org/military/system/munition/explosives-anfo.htm
>
> ANFO, at http://en.wikipedia.org/wiki/ANFO

Differences in the preparation of ANFO explosive as well as the physical make-up of its components can introduce variability in TNT equivalency. These can be manifest as variability in the amount of absorbed water in the mixture, a lack of uniformity in mixing, differences in specific gravity, and the particular oxidizer and type of fuel oil used.

Because of the inherent variability in one or more of these factors, there is uncertainty as to the TNT equivalent mass that should be assumed for a terrorist attack. To provide a framework for assessing the blast parameters, we shall assume in the following that the probability $F_m(m)dm$ that a terrorist explosive attack will involve an explosive of TNT equivalent mass m in the interval (m, m+dm) has the shape of a normal probability distribution function with a mean m_o and a dispersion δm, We shall also assume that the truncated normal probability distribution is only nonzero for m larger than some minimum m_{min} and for m less than some maximum m_{max}.

Specifically,

$$F_m(m)dm = \begin{cases} C_m \exp[-(m-m_o)^2/(\delta m)^2]dm & \text{for } m_{min} < m < m_{max} \\ 0 \text{ otherwise} & \end{cases} \qquad [1a]$$

where the normalization constant is

$$C_m = (2/\pi^{1/2}\delta m)\,[\mathrm{Erf}((m_{max}-m_o)/\delta m) + \mathrm{Erf}((m_o-m_{min})/\delta m) \qquad [1b]$$

From the foregoing discussion, we shall use as a numerical example

$$m_o = 32{,}000 \text{ lbs TNT}$$
$$m_{min} = 12{,}000 \text{ lbs TNT}$$
$$m_{max} = 64{,}000 \text{ lbs TNT}$$
$$\delta m = 20{,}000 \text{ lbs TNT} \qquad [2]$$

The mean value, 32,000 lbs, corresponds to 40,000 lb of ANFO with a TNT equivalency factor of 0.8, whereas the minimum and maximum values, 12,000 and 64,000 lbs, correspond to 40,000 lb of ANFO with TNT equivalency factors of 0.3 and 1.6, respectively. The dispersion $\delta m = 20{,}000$ lbs has been set equal to $m_o - m_{min}$ to describe a likely spread in values comparable to the difference between the nominal 0.8 equivalency factor and the minimum equivalency factor of 0.3. This spread has been chosen rather than a spread equal to the difference between the maximum equivalency factor of 1.6 and the nominal factor of 0.8, to weight more heavily the multitude of factors that can decrease the TNT equivalency.

The truncated normal probability distribution $F_m(m)$ is displayed in Figure 1 for the numerical parameters of eq. [2].

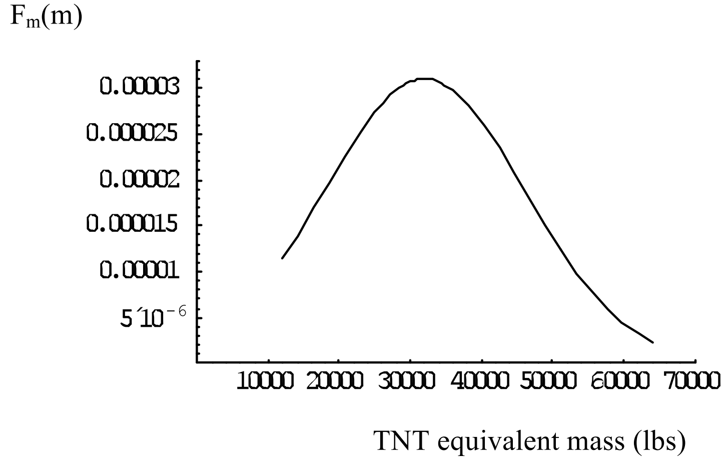

Figure 1. Probability function $F_m(m)$ for TNT equivalent mass m for the representative parameters of eq. [2].

2b. Uncertainty in Standoff Distance

Vehicle-borne explosive attacks represent a significant security concern and collateral damage experienced as a result of attacks against nearby facilities is a concern as well. This adds to the uncertainty associated with urban terrorist threats and thereby affects mitigation strategies under consideration. Strategically placed bollards will prevent a vehicle from ramming a facility as well as set a minimum vehicle access distance. We assume the closest distance of approach to a facility and still be within the iconic “orbit” of its intended target is 275 feet. Therefore, the standoff distance for a vehicle-borne explosive source should equal or exceed a 275 foot minimum.

However, a number of vehicle positions that border a target facility are equally likely from a terrorist’s perspective since any point along this border would inflict approximately the same damage to the target facility. However, differences in this distance could have a profound effect on collateral damage to neighboring facilities. The range of likely detonation positions relative to potential explosive damage to a neighboring facility is assumed to be principally dictated by the length of a street bordering the target building

Without further details of the terrorists' plans, we again resort to the normal probability distribution function as the one that best reflects the inherent uncertainty in key physical parameters. It should be noted that although a truncated normal distribution is most appropriate in this instance, the approach specified herein does not depend on the specific probability distribution. Since $F_m(m)$ and $F_r(r)$ are assumed to be independent, the joint probability and resulting contour plot could be calculated in similar fashion using alternative distribution functions. However, the dispersion associated with the chosen probability distributions which characterizes the uncertainty in potential threat scenarios is considered most important in calculating the probability of protection afforded by a given window design.

Specifically, we assume that the probability $F_r(r)dr$ that the standoff distance is between r and r+dr is also given by a truncated normal distribution:

$$F_r(r)dr = \begin{cases} C_r \exp[-(r-r_o)^2/(\delta r)^2]dr & \text{for } r_{min} < r < r_{max} \\ 0 \text{ otherwise} & \end{cases} \qquad [3a]$$

where the normalization constant is

$$C_r = (2/\pi^{1/2}\delta r)\ [\mathrm{Erf}((r_{max}-r_o)/\delta r) + \mathrm{Erf}((r_o-r_{min})/\delta r) \qquad [3b]$$

Here r_o denotes the value of the standoff distance at which the probability is largest: for example, when the detailed geometry of a target facility placement becomes available, this could be determined from the location of a vehicle that would place it as close as possible to the target. The dispersion δr measures the spread in likely values for the standoff distance. And as discussed earlier, r_{min} denotes the closest possible distance of approach to a neighboring facility and r_{max} denotes the maximum standoff distance from the neighboring facility for which an explosive-laden vehicle could do substantial damage to the target building.

To illustrate the approach, in the following we shall present a numerical example for

$$\begin{aligned} &r_{min} = 275 \text{ feet} \\ &r_{max} = 525 \text{ feet} \\ &r_o = 0.5\,(r_{min}+r_{max}) = 400 \text{ feet}) \\ &\delta r = r_o - r_{min} = 125 \text{ feet} \end{aligned} \qquad [4]$$

As more detailed information becomes available, these numbers can be modified.

The probability function $F_r(r)$ is displayed in Figure 2 for the numerical parameters of eq. [4].

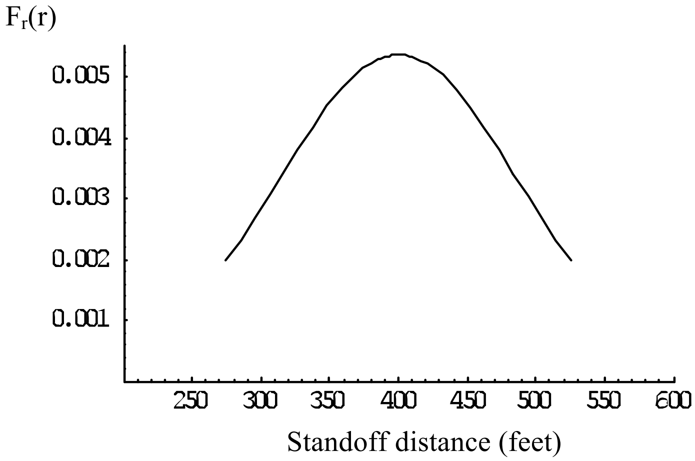

Figure 2. Probability function $F_r(r)$ for standoff distance r from a facility in proximity to the intended target for the representative parameters of eq. [4].

It is also of interest to look at the joint probability distribution function $F_{mr}(m,r)dmdr$ that gives the probability that the TNT equivalent mass m is in the range (m, m+dm) and the standoff distance is in the range (r,r+dr). Since we have assumed that the probability distribution functions of equations [1] and [2] are independent, we can write simply

$$F_{mr}(m,r) = F_m(m)\, F_r(r) \qquad [5]$$

The joint probability function $F_{mr}(m,r)$ is displayed in Figure 3 for the numerical parameters of eqs. [2] and [4]. As expected, the joint probability distribution function displays a single maximum at (m_o, r_o) with a spread in the TNT-equivalent mass m determined by δm and a spread in the standoff distance r determined by δr.

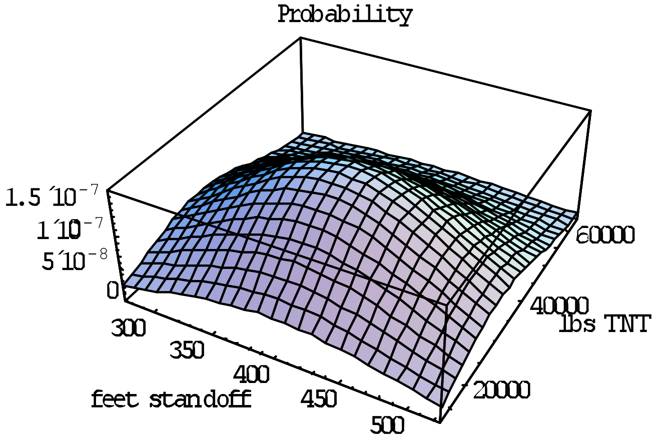

Figure 3 Joint probability function $F_{mr}(m,r)$ for the numerical parameters in eqs. [2] and [4]. In the 3D image of Figure 3a, the x-axis displays the TNT equivalent mass in lbs, and the y-axis displays the standoff distance in feet. In the contour plot of Figure 3b, the TNT equivalent mass is shown on the vertical axis and the standoff distance is shown on the horizontal axis.

The contour diagram of the probability function is shown in Figure 4.

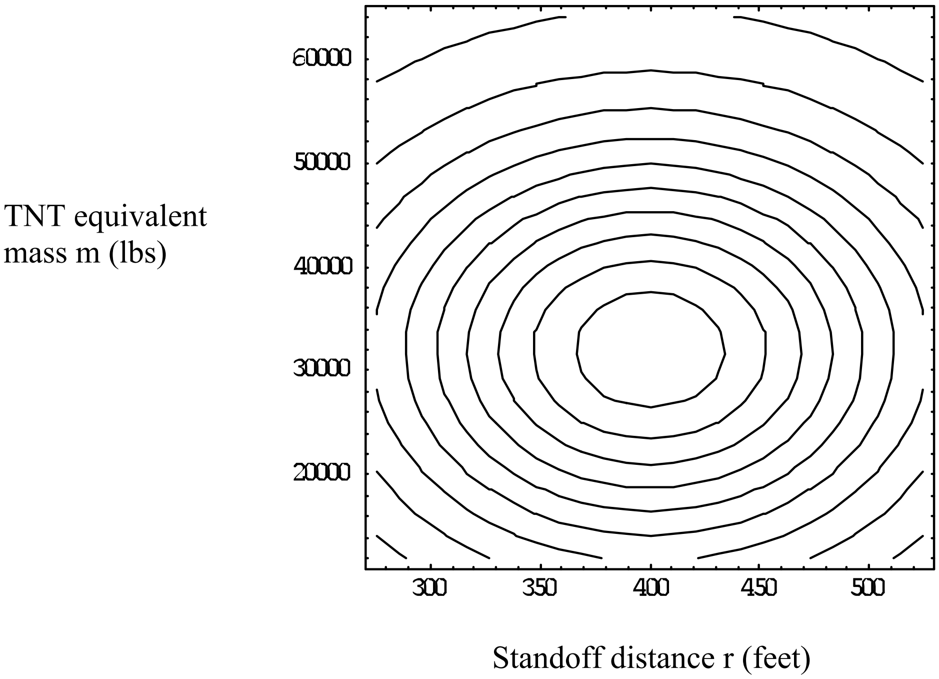

Figure 4. Contour plot of joint probability function $F_{mr}(m,r)$ for the numerical parameters in eqs. [2] and [4]. The TNT equivalent mass is shown on the vertical axis and the standoff distance is shown on the horizontal axis.

Finally, we note that a joint probability distribution could be calculated in this way for an unlimited number of physical parameters with an associated dispersion specified for each, assuming such parameters were independent. In this report, standoff distance and TNT equivalent mass were used since these directly affect overpressure and impulse as indicated in referenced scaling relations.

3. Structural damage from an explosive blast

In the preceding section we have discussed the probability distribution function $F_{mr}(m,r)dmdr$ for the TNT-equivalent mass m and the standoff distance r. The equivalent mass m and standoff distance r are not the explosive blast variables that are most directly related to structural damage. Rather, these variables are the blast overpressure p and the blast impulse I [See, e.g., M. Held, 1983]. In Section 4 we shall discuss how $p=p(m,r)$ and $i=i(m,r)$ are related to m and r. In this section, we shall briefly review why it is that blast overpressure p and blast impulse i are the quantities of most direct interest to determining structural damage.

The interaction of a blast wave with a structure is quite a complicated phenomenon. Ngo, Mendis, Gupta, and Ramsay (2007) have provided a recent overview of the problem.

At any point in the path of an explosive blast wave, the pressure rises rapidly to a maximum value that is known as the *overpressure*. This is followed by a slower – although still quite rapid - decay of the pressure to below the ambient pressure. During this decay to ambient pressure, an *impulse* is delivered to any object experiencing the increased pressure. This portion of the blast wave is then followed by a smaller drop in pressure below the ambient pressure and a more gradual return to atmospheric pressure. This portion can exert suction on an object, and can also deliver debris to the object that has been sucked into the blast wave.

In a crude analysis, the effect of a blast wave on a structure is related to the magnitude of the overpressure. Thus, in FEMA and DOD documents, tables similar to Table 1 are often displayed. Table 1, taken from the DOD document TB 700-2 (cited in Jeremic and Bajic, 2006), lists the types of damage to be expected from various blast overpressures.

Table 1. Expected shock wave effects on objects (from DOD's TB 700-2, cited in Jeremic and Bajic, 2006). - psi units added

No.	Overpressure		Expected damage
	kPa	psi	
1	1.0-1.5	0.15-0.22	Window glass cracks
2	3.5-7.6	0.51-1.1	Minor damage in some buildings
3.	7.6-12.4	1.1-1.8	Metal panels deformed
4.	12.4-20	1.8-2.9	Concrete walls damage
5.	Over 35	Over 5.1	Wooden construction buildings demolition
6.	27.5-48	4.0 -7.0	Major damage on steel construction objects
7.	40-60	5.8-8.7	Heavy damage on reinforced concrete buildings
8.	70-80	10-11.6	Probable demolition of most buildings

However, the duration of the pressure pulse in the blast also plays a role in determining damage, i.e. the damage is related to the impulse as well as to the overpressure. An example of this is given in Figure 5, based on a figure from DOD's TM15-1300 (cited in Ngo, Mendix, Gupta, Ramsay, 2007). Figure 5 shows a design chart for a tempered glass panel. It shows clearly that the survival of a panel depends not just on the peak pressure but also on the blast impulse to which it will be subjected.

The reason why both overpressure and impulse are important in determining structure damage becomes evident in a simple model that is sometimes used to describe blast wave/structure interaction: In this model - the so-called single degree if freedom (SDOF) model - the structure (or an element of the structure) is replaced by an equivalent system of one concentrated mass and one weightless spring that represents the resistance of the structure to deformation.

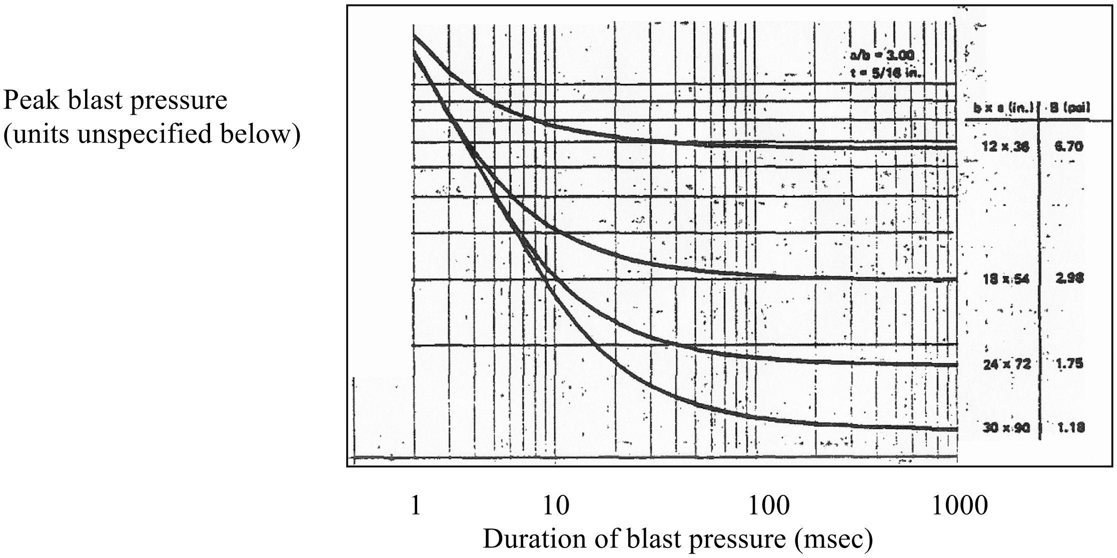

Figure 5. A design chart for a tempered glass panel (TM5-1300, Figure 6-43).
It displays the peak pressure that different panels can withstand as the blast duration is varied.

It is well known that the response of a mass on a spring to a transient force is qualitatively different when the natural oscillation period (determined by the spring constant and the mass) is greater than the force duration than when it is less than the force duration. In the former, the impulse (the integral of the force over time) determines the initial velocity of response of the mass, while in the latter the displacement of the mass is practically proportional to the force throughout its application. In a building, different elements of the building will have different natural oscillation frequencies, and the response of any particular element in its surroundings will respond accordingly either to the blast overpressure exerted on it or to the blast impulse.

In Ngo, Mendix, Gupta, Ramsay, 2007, a half dozen computer programs are listed that are used for calculating structural responses and for designing blast-resistant structures.

4. Scaling laws for blast overpressure and impulse

Several approximate scaling laws have been suggested in the literature to relate blast overpressure and impulse - the variables of interest for determining structural damage – to the TNT-equivalent mass and standoff distance of the explosive. Several examples are listed below:

Overpressure

- **M.A. Sadovski** [cited in Jeremic and Bajic, 2006]

  $p(m,r) = 0.085(m^{1/3}/r) + 0.3(m^{2/3}/r^2) + 0.8(m/r^3)$ MPa [6]

- **H.L. Brode (1955)**

$p(m,r) = 0.1 + 0.67\ (m/r^3)$ MPa for $p(m,r) > 1$ MPa [7a]

$p(m,r) = 0.0975(m^{1/3}/r) + 0.1455(m^{2/3}/r^2) + 0.585(m/r^3) - 0.0019$ MPa

for $0.01 < p(m,r) < 1$ MPa [7b]

- **C.A. Mills (1987)**

$p(m,r) = 0.108(m^{1/3}/r) - 0.114(m^{2/3}/r^2) + 1.772(m/r^3)$ MPa [8]

- **M. Held (1983)**

$p(m,r) = 2(m^{2/3}/r^2)$ MPa [9]

Impulse

- **M.A. Sadovski** [cited in Jeremic and Bajic, 2006]

$i(m,r) = 200(m^{2/3}/r)$ Pa-s [10]

- **M. Held (1983)**

$i(m,r) = 300(m^{2/3}/r)$ Pa-s [11]

Note: In these expressions, the TNT-mass equivalent m is expressed in kg and the standoff distance r is expressed in meters

It is interesting to see how varied the scaling laws for overpressure are, and how not many scaling laws have been proposed for the impulse. This is a reflection of the complex nature of the explosive blast wave.

For example, the impulse depends strongly on the shape of the decaying pressure pulse following the large overpressure due to the blast shock wave. Multiplication of the overpressure by cited durations for the pressure pulse do not give good approximations for the impulse.

In the following we shall use Sadovski's expressions for both the overpressure and the impulse, i.e. we shall use eq. [6] for p(m,r) and eq. [10] for i[m,r]. Sadovski based his scaling laws on numerous experimental results; and in addition, for the range of overpressures of interest, comparisons of the shapes of actual data curves with curve fitting expressions seem to favor expressions containing multiple terms [See, e.g., G.F. Kinney (1962)].

Equations [6] and [10] are rewritten below in units of psi, psi-msec, lbs, and ft

$p(m,r) = 31.11(m^{1/3}/r) + 276.9(m^{2/3}/r^2) + 1863(m/r^3)$ psi for m in lbs and r in ft [6]

$i(m,r) = 56.25(m^{2/3}/r)$ psi msec for m in lbs and r in ft [10]

The blast overpressure p(m,r) given by eq. [6] as a function of TNT equivalent mass m and standoff distance r is displayed in Figure 6. Figure 7 shows the blast impulse i(m,r) given by eq. [10].

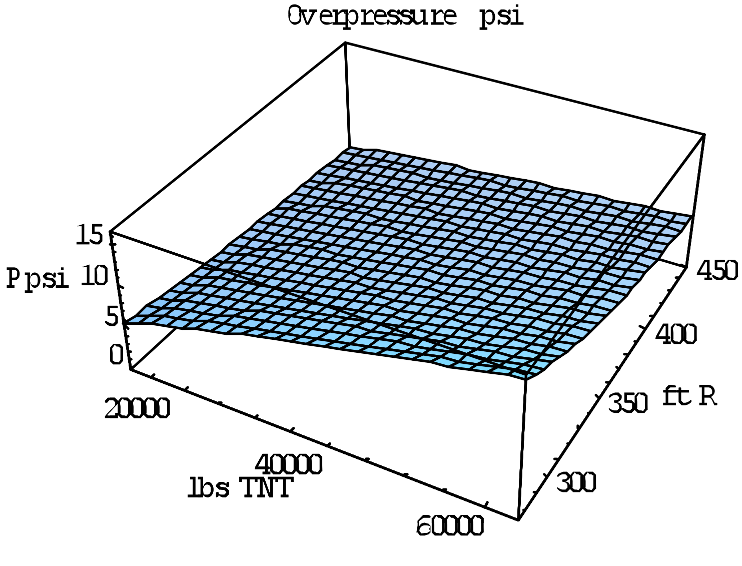

Figure 6. Blast overpressure p(m,r) as a function of TNT equivalent mass m and standoff distance r, from eq. [6]. The z-axis shows the overpressure p(m,r) in psi. The x-axis shows the TNT-equivalent mass m in lbs, and the y-axis shows the standoff distance in feet.

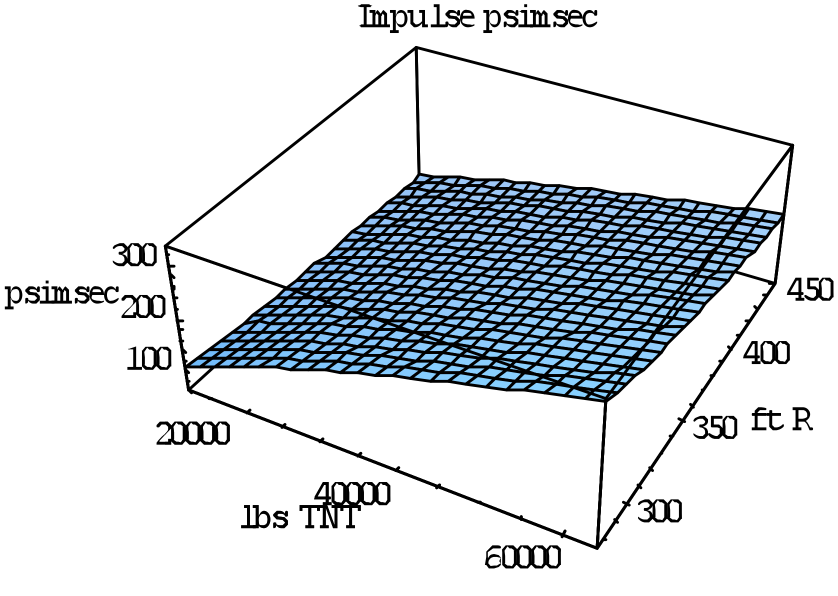

Figure 7. Blast impulse i(m,r) as a function of TNT equivalent mass m and standoff distance r, from eq. [10]. The z-axis shows the impulse i(m,r) in psi msec. The x-axis shows the TNT-equivalent mass m in lbs, and the y-axis shows the standoff distance in feet.

It is also of interest to solve eqs. [6] and [10] for TNT-equivalent mass m in terms of blast overpressure p and impulse i, as well as for standoff distance r in terms of p and i. The solutions for m(p,i) and r(p,i) are rather messy algebraically, but can be obtained straightforwardly with Mathematica symbolic algebra software. This yielded three possible roots each for m(p,i) and r(p,i) where two of the three are complex and therefore nonphysical.

The dependence of the standoff distance r(p,i) on overpressure p and impulse i is shown in Figure 8, whereas Figure 9 shows how the TNT-equivalent mass m(p,i) depends on p and i.

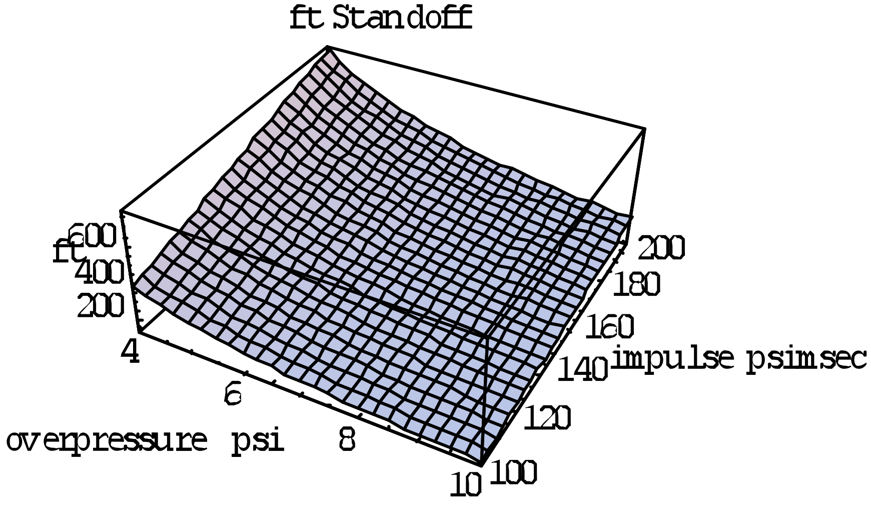

Figure 8. Standoff distance r as a function of overpressure p and impulse i. The standoff distance is shown along the z-direction in feet, with the overpressure shown along the x-axis in psi and the blast impulse shown along the y-axis in psi msec.

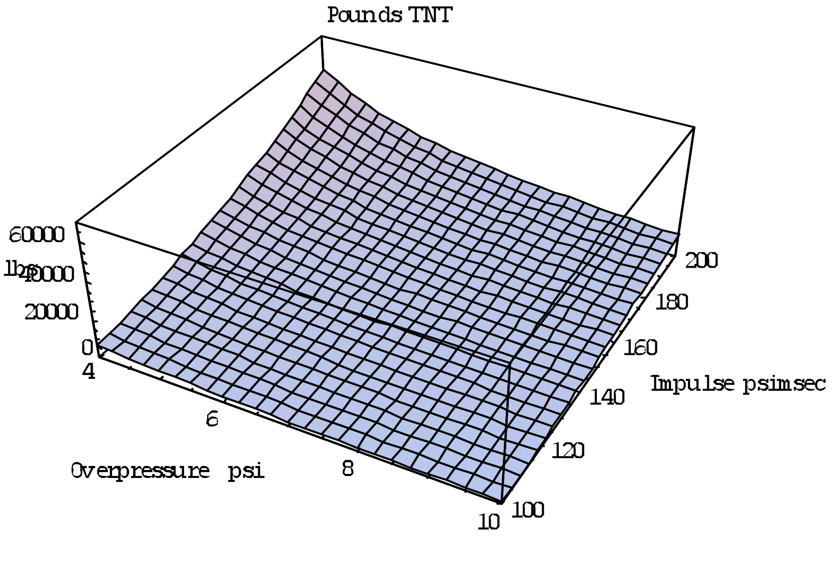

Figure 9. TNT-equivalent mass m as a function of overpressure p and impulse i. The TNT-equivalent mass is shown along the z-direction in lbs, with the overpressure shown along the x-axis in psi and the blast impulse shown along the y-axis in psi msec.

The plots show that the largest values for standoff distance r and TNT-equivalent mass m occur when the overpressure, p, is small and the impulse, i, is large.

5. Design curves for blast protection

In order to obtain an estimate for the degree of blast protection, the probability considerations need to be combined with a design curve that sets the limits of integration for the probability function.

Simple SDOF model For calculating the response of a structure such as a window to a blast wave, an approximation that is sometimes used is to replace the components of the structure by a simple mass M held in place by a spring of spring constant K. This approximation is termed the single degree of freedom (SDOF) approximation.

The displacement y(t) of the mass in response to a time dependent force F(t) is obtained from the equation

$$d^2y/dt^2 + \omega^2 y = F/M \qquad [11]$$

where the natural oscillation angular frequency ω is given by $\omega^2 = K/M$. If the force is due to a transient pressure pulse P, we can further write $F= PA$ where A is the area of the component.

Suppose we characterize the transient pressure pulse by the crude approximation

$$P(t) = \mathrm{P}\exp(-t/T) \qquad [12]$$

The impulse associated with this is I = PT
Then, assuming that the initial displacement and velocity of the component are zero, the solution is simply

$$y(t) = \alpha[\exp(-t/T) -\cos(\omega t) +(1/(\omega T\sin(\omega t))] \qquad [13]$$

where

$$\alpha = (PA/M)I^2/(P^2+(\omega I)^2) \qquad [14]$$

The design curve can be obtained by setting the maximum value of y(t), i.e., where dy/dt = 0, equal to a critical displacement y_c, sometimes taken as 1/175 of the linear dimension of the component [http://en.wikipedia.org/wiki/Curtain_wall].

Design curve equations in dimensionless variables This then leads to the equations:

$$\exp(-xp/i) = (1/p) +\cos x \qquad [15]$$

$$\sin x = 1/i \qquad [16]$$

where the dimensionless variables p and i have been introduced. They are related to the actual overpressure P and impulse I by

$$p = P_0/\omega^2\chi \qquad [17]$$

$$i = I/\omega\chi \qquad [18]$$

where

$$\chi = y_c M/A \qquad [19]$$

The solution of eqs. [18] and [19] are shown in Figure 10. It was obtained by numerical solution.

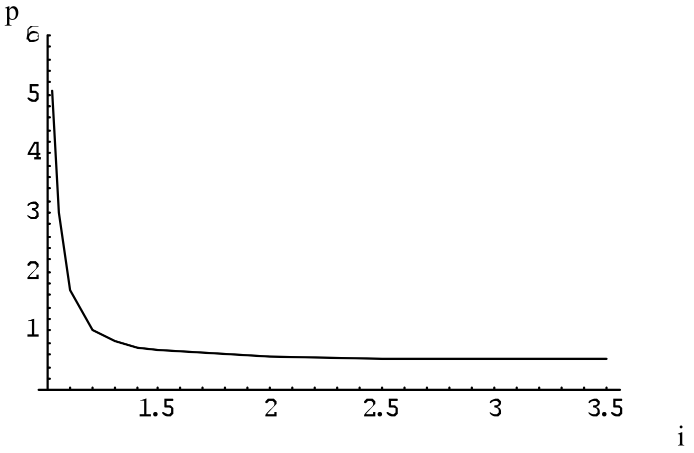

Figure 10. SDOF design curve obtained from eqs. [18] and [19] for the dimensionless variables p and i. The dimensionless variables are related to the actual overpressure and impulse by $p = P/\omega^2\chi$, $i = I/\omega\chi$, where $\chi = y_c M/A$ is related to the critical displacement, mass, and component area.

The design curve displays two asymptotes, one for p>>1 and i approaching 1, and the other for i>>1 and p approaching ½. It is easy to see from eqs. [18] and [19] that the asymptotic behaviour is described by

$$p \approx [1-(1/i^2)]^{-1/2} \qquad \text{when } p>>1 \qquad [20]$$

$$p \approx ½ + (\pi/8)(1/i) \qquad \text{when } i>>1 \qquad [21]$$

The design curve of Figure 10 in the dimensionless variables p and i is a universal curve: it applies whenever a structural component can be represented by a SDOF mass attached to a spring.

Design curve in actual overpressure and impulse To relate the design curves in the dimensionless variables to the design curves for an actual situation, the natural angular oscillation frequency ω of the system and the parameter χ must be known.

As an example, suppose we take the natural period of the system to be 0.11 sec. ($\omega = 56 \text{ sec}^{-1}$). This is in the range of the values shown in a specific report provided by an explosives consultant. In addition, let us take the curve to pass through the design point: 8 psi and 170 psi msec.

From eqs. [20]&[21] we see that for a design point (P_d,I_d), the corresponding point (p_d,i_d) in the dimensionless space satisfy the relation

$$P_d/I_d = \omega\ (p_d/i_d) \qquad [22]$$

With the choice of the natural oscillation frequency of 56 sec^{-1} along with the design point ($P_d = 8$ psi and $I_d = 170$ psi msec = 0.17 psi sec), eq. [25] requires $p_d/i_d = 0.84$. From Figure 10, it can be seen that $p_d = 1.01145$ and $i_d = 1.2$. For this example, then,

$$\chi = I_d/i_d\ \omega = 0.0025 \qquad [23]$$

Accordingly

$$P = 8 \text{ psi} \qquad [24]$$

$$I = 142 \text{ psi-msec} \qquad [25]$$

This design curve is shown in Figure 11.

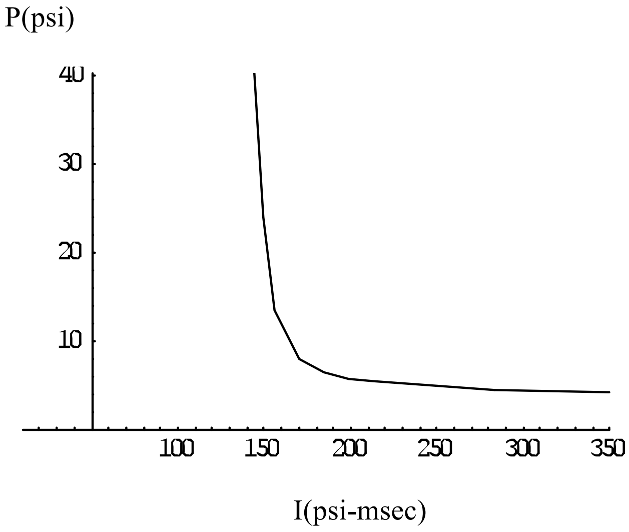

Figure 11. Design curve passing through 8 psi and 170 psi msec for a natural oscillation angular frequency of 56 sec^{-1}.

As another example, suppose instead the design point is taken to be 16 psi and 185 psi msec, and the natural oscillation angular frequency remains at 56 sec^{-1}. The same procedure leads in this case to

$$P = 9.42\ p \quad \text{psi} \qquad [26]$$
$$I = 168\ i \quad \text{psi-msec}$$

The resulting design curve for 16 psi and 185 psi msec is shown in Figure 12 (dashed) and compared to the design curve of Figure 10 for 8 psi and 170 psi msec.

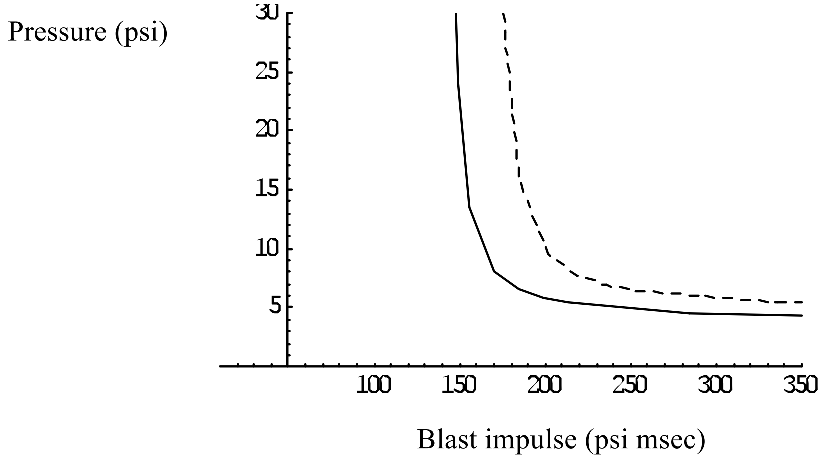

Figure 12. Design curves for blast protection. The solid curve is chosen to pass through 8 psi and 170 psi msec for a natural oscillation angular frequency of 56 $\sec^{-1}$. The dashed curve is chosen to pass through 16 psi and 185 psi msec, with the same natural oscillation angular frequency of 56 $\sec^{-1}$.

Design curve translated into (r,m) space The level of blast protection depends on the particular design curve chosen. In the next section, the design curves will be combined with the probability function discussed in Section 2 to obtain a confidence level for blast protection. For that purpose, it will be convenient to transform the design curves depicted in Figure 12 in the (overpressure, impulse) plane to the (equivalent TNT mass m, standoff distance r) plane. This can be done using eqs. [12] and [13]. Figure 13 displays the design curves of Figure 12 in the (m,r) plane.

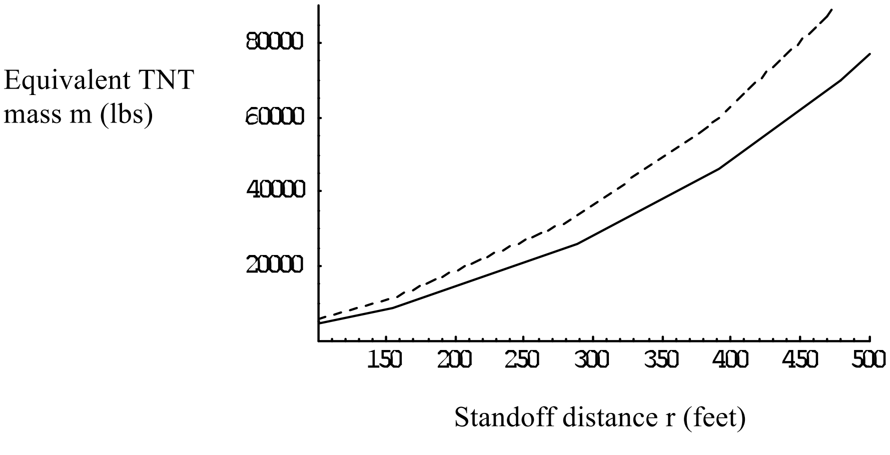

Figure 13. Design curves for blast protection. These are the same design curves as in Figure 12, but plotted here in the (m,r) plane. The solid curve is chosen to pass through 8 psi and 170 psi msec for a natural oscillation angular frequency of 56 $\sec^{-1}$. The dashed curve is chosen to pass through 16 psi and 185 psi msec, with the same natural oscillation angular frequency of 56 $\sec^{-1}$.

6. Probability of blast protection

The significance of a design curve in Figure 13 is that the associated structural component is protected from any blast for which the TNT equivalent mass and standoff distance gives a point lying under the curve. Accordingly, the probability that the component will withstand a blast is obtained by integrating the probability function over all points (m,r) that lie underneath the curve.

The design curves of Figure 13 are almost linear through the portion of the region they occupy where the probability function is zero. Linear fits to the curves in this portion are shown superimposed on the contour diagram for the probability function (of Figure 4), in Figure 14. The curves are shown only in the range of m and r where the probability function is nonzero.

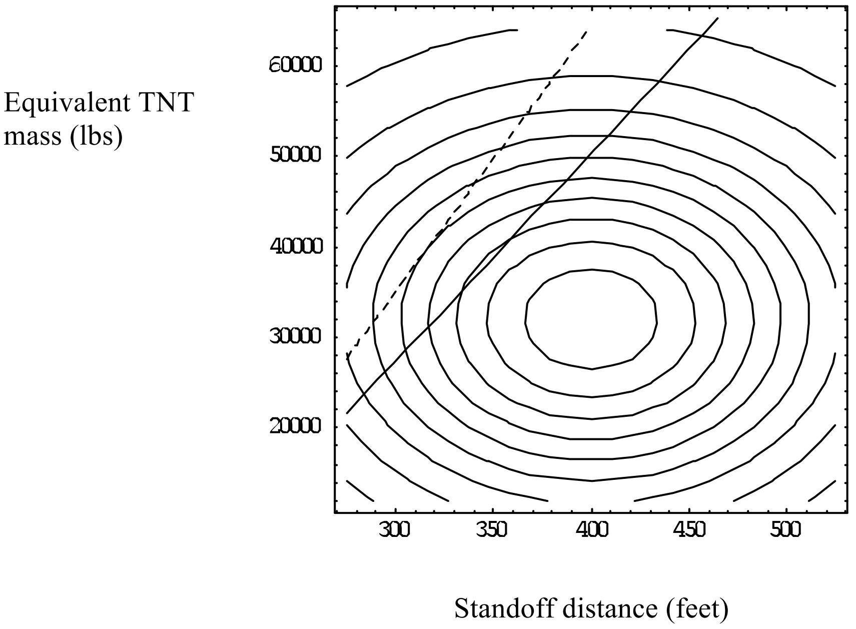

Figure 14. Design curves of Figure 13 superimposed on the probability function contour diagram of Figure 4. Again, the solid design curve is chosen to pass through 8 psi and 170 psi msec for a natural oscillation angular frequency of 56 sec^{-1}, whereas the dashed curve is chosen to pass through 16 psi and 185 psi msec, with the same natural oscillation angular frequency of 56 sec^{-1}. The probability function $F_{mr}(m,r)$ is given by eq. [5] as the product of truncated normal distributions in m and r.

For both design curves, it is seen that the maximum of the probability function lies below design curves. It is also seen that more of the probability function is below the dashed curve (16 psi, 185 psi msec design) than below the solid curve (8 psi, 170 msec). Thus, it would be expected that the confidence level for protection for the former would be higher than for the lower.

For the design curves depicted in Figure 14, the probability $P_{protected}$ that the structural component will be protected against a blast is

$$P_{protected} = \int_{r_{min}}^{r_{ma}} dr \int_{m_{min}}^{\text{smaller of } \{m_{design}(r),\, m_{max}\}} F_{mr}(m,r)\, dm \qquad [27]$$

where $m_{design}(r)$ denotes the design curve. For the two representative design curves of Figure 14, this integration gives:

$P_{protected}$ (8 psi, 170 psi msec, 56 sec^{-1} design) = 80%

$P_{protected}$(16 psi, 185 psi msec, 56 sec^{-1} design) = 91%

i.e., the probabilities of blast protection for the two designs are **80%** and **91%,** respectively.

7. Summary and discussion

7a. Summary

A probabilistic risk assessment procedure has been followed to estimate the level of blast protection at a facility. We have assumed that the damage would be collateral, with the principal terrorist target being a nearby facility. A probabilistic approach was adopted because there are uncertainties associated with both the TNT-equivalent mass of the explosive and with the standoff distance of the detonation. These uncertainties in explosive mass and standoff distance translate through commonly used scaling laws into uncertainties in the blast wave overpressures and impulses. The overpressures and impulses are of more direct interest to structural designers.

Normal distributions, with cutoffs at reasonable minimum and maximum values, have been assumed for both the TNT equivalencies of the charge and the standoff distances [Figure 3]. A structural component design curve for blast mitigation has been derived from an oft-used simple single degree of freedom (SDOF) model. This design curve defines the boundary between the overpressures and impulse combinations from which the structural component will be protected and those for which the design affords no protection. Use of the scaling laws translates this information into a boundary between combinations of TNT-equivalent mass and standoff distance. The probability of protection is then obtained by integrating the normal probability distributions over all masses and distances that lie on the protected side of the design curve.

Two numerical examples have been given, both for a structural component that has a natural oscillation period of 0.11 sec, corresponding to a natural oscillation angular frequency of 56 sec^{-1}. In the first example, the design curve has been chosen to pass through the point (8 psi, 170 psi msec); the resulting probability of protection is 80%. In the second example, the design curve has been chosen to pass through the point (16 psi, 185 psi msec): the resulting probability of protection for this case is 91%. Thus, the first example gives protection at the 1.3-sigma level, whereas the second example provides protection at the 1.7-sigma level.

7b. Discussion

This report has focused on deriving the probability of protection afforded by a specific window design as a result of an explosive blast.

It should be noted that as more information is known about risk mitigation such as the emplacement of bollards to enforce standoff, the geometry of a target facility relative to the surrounding streets, and likely screening procedures, improvements can be made on the normal truncated probability distributions assumed for TNT-equivalent masses and standoff distances.

In addition, we believe that the probabilistic approach in this report and applied to a specific terrorist-initiated explosive threat can find application in a much broader range of operational risk problems. A general four-step process is envisioned:

1. The starting point is to assume an appropriate probability function (often a normal distribution) for a set of parameters that is inherently random, and that have some (indirect) connection with the mitigation.

2. The second step is to develop equations (scaling laws) that relate these inherently random parameters to a second set of parameters that most directly impact the mitigation under consideration.

3. The third step is to identify design curves (or surfaces) for a group of selected risk-aversion measures in the second set of parameters.

4. The fourth step is to use identified scaling laws to map the design curves (surfaces) onto the space of inherently random parameters, and to integrate the normal probability function over that portion of the space that is protected by the mitigation design. This then gives the probability that the applied mitigation will be successful, i.e. it provides statistical confidence in a successful implementation.

Alternatively, steps 3 and 4 can be replaced by:

3 (alternate). The third step is to use the results of the first two steps to generate a probability distribution for the second set of parameters.

4 (alternate). The fourth step is to integrate the probability function over the portion of the space of the second set of parameters that is defined by the design curves (surfaces) for selected risk mitigation measures. This then gives the probability that the risk mitigation will be successful.

The choice between Steps 3 and 4 or the alternate Steps 3 and 4 could be based on the relative ease of calculation for the two options in a given risk scenario.

The approach can be used to systematically estimate the effectiveness of mitigation measures and associated costs required to achieve varying degrees of protection.

References

ANFO, at http://en.wikipedia.org/wiki/ANFO

Brode, H.L., Numerical solution of spherical blast waves, J App Phys **26**, 766-775 (1955)

Explosives – ANFO *Ammonium nitrate-fuel oil), at http://www.globalsecurity.org/military/system/munition/explosives-anfo.htm

Held, M., Blast waves in free air, Propellants, Explosives, Pyrotechnics **8**, 1-7 (1983)

Jeremic, R., and Bajic, Z., An approach to determining the TNT equivalent of high explosives, Scientific-Technical Review **56**, 58-62 (2006)

Kinney, Gilbert F., **Explosive Shocks in Air**. N.Y.: The MacMillan Co. (1962)

Mills, C.A., The design of concrete structure to resist explosions and weapon effects, Proceedings of the 1st Intl. Conf. On concrete for hazard protections, Edinburgh, UK, 61-73 (1987)

Netherton, N.D., and Stewart, M.G., The effects of explosive blast load variability on safety hazard and damage risks for monolithic window glazing, International Journal of Impact Engineering, 36 (2009) 1346-1354

Newmark, N.M., and Hansen, R.J., Design of blast resistant structures, Shock and Vibration Handbook **3**, eds. Harris, C.M., and Crede, C.E.. N/Y.: McGraw-Hill (1961)

Ngo, T., Mendis, P., Gupta, A., and Ramsay, T., Blast loading and blast effects on structures – an overview, EJSE Special issue: Loading on structures, 76-91 (2007)

Stewart, M.G., Netherton, M.D., Rosowsky, D.V., Terrorism risks and blast damage to built infrastructure, Natural Hazards Review **7**, 114-122 (2006)

TB 700-2, NAVSEAINST 8020.8 B, DOD Ammunition and Explosives Hazards Classification Procedures, Washington DC (1999)

TM 5-1300, The Design of Structures to Resist the Effects of Accidental Explosions, Technical Manual, US Department of the Army, Navy, and Air Force, Washington DC, 1990

Viewpoint Paper

Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities*

Roger G. Johnston
Vulnerability Assessment Team
Nuclear Engineering Division
Argonne National Laboratory

The following ideas are common, but I think quite wrong and thus myths:

(1) A Threat without a mitigation is a Vulnerability.

(2) A Threat Assessment (TA) is a Vulnerability Assessment (VA).

(3) Threats are more important to understand than Vulnerabilities.

(4) Many of the most common tools used for "Vulnerability Assessments" (whether true VAs or actually TAs) are good at finding Vulnerabilities.

First some definitions. Most security professionals would probably more or less agree with the following definitions:

Threat: Who might attack against what assets, using what resources, with what goal in mind, when/where/why, and with what probability. There might also be included some general aspect of the nature of the attack (e.g., car bombing, theft of equipment, etc.), but not details about the attack or the security measures that must be defeated and the Vulnerabilities to be exploited.

Threat Assessment (TA): Attempting to predict the Threats. This may involve using intelligence data and information on past security incidents (at this building, facility, or infrastructure or ones like it.) To have proactive (not just reactive) security, however, a valid TA requires anticipating Threats that have not yet materialized.

*Editor's Note: This paper was not peer-reviewed. This work was performed under the auspices of the United States Department of Energy (DOE) under contract DE-AC02-06CH11357. The views expressed here are those of the author and should not necessarily be ascribed to Argonne National Laboratory or DOE. Jon Warner provided useful suggestions.

Vulnerability: a specific weakness in security (or a lack of security measures) that typically could be exploited by multiple adversaries having a range of motivations and interest in a lot of different assets.

Vulnerability Assessment (VA): Attempting to discover (and perhaps demonstrate) security Vulnerabilities that could be exploited by an adversary. A good VA also often suggests practical countermeasures or improvements in security to eliminate or mitigate the Vulnerability, or to aid in resiliency and recovery after an attack.

Risk Management: Attempting to minimize (security) hazards by deciding intelligently how to deploy, modify, or re-assign security resources. Involves the following inputs: TA results, VA results, assets to be protected, consequences of successful attacks, and the resources (time, funding, personnel) available to provide security.

Attack: An attempt by an adversary to cause harm to valuable assets, usually by trying to exploit one or more Vulnerabilities. The harm may include theft, sabotage, destruction, espionage, tampering, or adulteration.

Some examples of Threats and Vulnerabilities.

Threat: Adversaries might install malware in the computers in our Personnel Department so they can steal social security numbers for purposes of identity theft.
Vulnerability: The computers in the Personnel Department do not have up to date virus definitions for their anti-malware software.

Threat: Thieves could break into our facility and steal our equipment.
Vulnerability: The lock we are using on the building doors is easy to pick or bump.

Threat: Nefarious insiders might release confidential information to adversaries.
Vulnerability: Employees don’t currently have a good understanding of what information is sensitive/confidential and what is not, so they can’t do a good job of protecting it.

Threat: Disgruntled employees could sabotage our facility.
Vulnerability: The organization lacks effective Insider Threat countermeasures like background checks and disgruntlement mitigation (fair treatment of

employees, legitimate complaint resolution processes, employee assistance programs, no tolerance for bully bosses, etc.)

Threat: Extremists want to discredit our organization.
Vulnerability: It is easy for them to dump hazardous chemicals on our property or pour them down our drains, and then fraudulently report us to the authorities as polluters.

With these definitions, it should be clear that myth #1 above ("a Threat without a mitigation is a Vulnerability") makes no sense because (a) a Threat is not a Vulnerability, (b) security is a continuum and 100% elimination of a Vulnerability is rarely possible, (c) adversaries may not automatically recognize a Vulnerability so mitigating it may be irrelevant for that specific Threat, and (d) Vulnerabilities don't define Threats, i.e., terrorists don't exist because buildings and people can be blown up.

The commonly held myth #2 (TAs are VAs) is untrue because Threats are not the same thing as Vulnerabilities. Both TAs and VAs are needed, however, for good Risk Management, and they both depend on each other to some extent. Adversaries typically seek to exploit Vulnerabilities. Indeed, if there were no Vulnerabilities, the adversaries won't succeed. And if there were no Threats, any existing security Vulnerabilities would be irrelevant.

Note that Vulnerabilities don't map one-to-one onto Threats. Many different kinds of adversaries with very different agendas can potentially exploit the same Vulnerability for very different reasons. Thus a lock that is easy to pick permits attacks involving theft, espionage, or vandalism. Computers lacking up to date virus checkers can be exploited for lots of different nefarious purposes. Of course, Threats don't map one-to-one onto Vulnerabilities, either. An adversary can potentially pick and choose which Vulnerability or Vulnerabilities to exploit for any given goal.

In thinking about Myth #3 (Threats are more important than Vulnerabilities) we need to consider that a TA involves mostly speculating about people who are not in front of us, and who might not even exist, but who have complex motivations, goals, mindsets, and resources if they do exist. Vulnerabilities are more concrete and right in front of us (if we're clever and imaginative enough to see them). They are discovered by doing an analysis of actual infrastructure and its security—not speculating about people. Thus, getting Threats right is typically a lot harder than getting Vulnerabilities right. [Some people claim that past security incidents can tell us all we need to know about Threats, but that is just being reactive, not proactive, and misses rare but very catastrophic attacks.]

I would go even further and argue that understanding Vulnerabilities is more powerful than understanding Threats—regardless of the relative difficulty of TAs vs. VAs. If you understand and take some reasonable effort to mitigate your security Vulnerabilities, you are probably in fairly good shape regardless of the Threats (which you are likely to get wrong anyway). On the other hand, if you understand the Threats but are ignorant of the Vulnerabilities, you are not likely to be very secure because the adversaries will have many different ways in.

Myth #4 (existing tools are effective at finding Vulnerabilities) is quite prevalent, especially for infrastructure security. This is perhaps because there are such a staggering number of Vulnerabilities in any large, complex system (especially compared to Threats) that dealing with the Vulnerabilities is daunting. Also, finding Vulnerabilities takes a lot of careful thinking, on the ground investigation, hands-on analysis, and imagination/creativity. Threat Assessments, in contrast, often (unfortunately) involve relatively easy and simple-minded use of check lists, security surveys, compliance audits, guidelines, software programs, boilerplates, compliance requirements, databases of past security incidents, and “cookie cutter” approaches. There is, of course, no reason why a TA can’t or shouldn’t involve profound, critical, original, and creative thinking about security issues, it’s just that is so often does not.

I break down the so-called “Vulnerability Assessment” methods into 4 general categories:

1. Tools that can help find vulnerabilities but aren’t typically very good at it because they do not encourage thinking creatively like the bad guys about actual, local vulnerabilities and/or they make invalid assumptions: Security Surveys, Compliance Audits, boilerplate Software Programs, Tree Analysis, “Red Team” exercises.

2. Tools that are good at finding Vulnerability Assessments: Adversarial Vulnerability Assessments (thinking about the security problem from the perspective of the bad guys, not the good guys and the existing security implementation), intrusion testing programs (for cyber security), critical security design reviews early in the design process for new security devices, systems, or programs.

3. Misnamed "Vulnerability Assessment" tools that are really techniques for helping to decide how to allocate security resources, i.e., more like overall Risk Management than VAs *per se*: CARVER Method, Delphi Method.

4. Tools that (despite the claims) are actually TA methods, not VA methods: Design Basis Threat, Compliance Audits, boilerplate Software Programs.

One litmus test to tell if somebody claiming to do a Vulnerability Assessment is really doing a Threat Assessment is if they have identified a relatively small number of "Threats/vulnerabilities" (which they typically put in a table with made up rankings or probabilities), and if mitigating them is a major undertaking. If they are really doing a VA, they will have identified and maybe demonstrated dozens or hundreds of very specific vulnerabilities, and many of the countermeasures for mitigating them will be cheap and relatively painless, e.g., install anti-virus software in the Personnel Department computers that automatically updates virus definitions.

Another sort of related problem commonly found in infrastructure security assessments is confusing features with vulnerabilities. Thus, a public road that travels close to the facility is often considered a Vulnerability. It is not, however; it is only an attribute. Only when coupled with an attack scenario (truck bomb, the road makes visual and electronic surveillance easier for espionage, assets can be thrown over the fence by insiders to the bad guy's parked truck, etc.) does a feature become a Vulnerability. The reason this is important is that different kinds of security countermeasures will typically be needed for different combinations of feature + attack. Without the context of attack scenarios, the only apparent countermeasure is to eliminate the feature; this may be expensive, impractical, and/or total overkill.

Finally, we should not get confused about the purpose of a TA or VA. Neither a Threat Assessment or a Vulnerability Assessment is something we test against, some kind of "certification", a standard, a metric for how good our security is, or a technique for finding out if our security mangers or frontline personnel are screwing up. The purpose of a VA is to improve security. The purpose of a TA is to help us decide (in conjunction with Risk Management) what and how much security we need. It doesn't make any sense to talk about "passing" a TA or VA. This certainly cannot mean all Threats have been recognized or neutralized, or that there are zero Vulnerabilities or even that all Vulnerabilities are known and mitigated. Such things are not possible, and not provably true even if they were possible.

Viewpoint Paper

Changing Security Paradigms*

Roger G. Johnston
Vulnerability Assessment Team, Nuclear Engineering Division
Argonne National Laboratory

Any field is molded and constrained by its paradigms. A "paradigm" can be defined as:
(1) a pattern, example, or model;
(2) a mode of thought or practice;
or
(3) an overall concept or strategy accepted by most people in a given field.

The field of security relies on a number of paradigms, both stated and unstated. Many of these are in the process of changing—or at least should change—in order to adapt to a rapidly changing world and to improve security effectiveness.

This paper offers a brief, bulleted list of some security paradigms that I believe (perhaps currently more out of wishful thinking than empirical evidence) are in the process of changing. The new paradigms I identify here will, I believe, ultimately win out in the end over the old paradigms because they will result in better security. In my view, these emerging changes are worth monitoring and even carefully researching.

Security Paradigm 1 (The Nature of Security)

Old Paradigm:
- Security is binary: an asset is either secure or it is not.
- Check Box mentality.
- There is a minimum level of adequate security and we know what it is.
- There's a right way to do security, and there shouldn't be a lot of questioning.

New Paradigm:
- Security is a continuum, not black & white.
- Nobody knows how much security is "enough".
- Everything is a tradeoff.
- Security should be controversial and open for debate, as should any challenging, complex and important responsibility.

* Editor's Note: This paper was not peer-reviewed. This work was performed under the auspices of the United States Department of Energy (DOE) under contract DE-AC02-06CH11357. The views expressed here are those of the author and should not necessarily be ascribed to Argonne National Laboratory or DOE.

Security Paradigm 2 (Vulnerabilities)

Old Paradigm:
- Find all the vulnerabilities and eliminate them.
- Vulnerabilities are bad news.

New Paradigm:
- There are too many vulnerabilities to find them all, much less eliminate them all.
- Try to find those that are easiest to exploit, most likely to be exploited, and/or easiest to fix.
- We must still manage the vulnerabilities we haven't eliminated, or know nothing about.
- Finding a vulnerability is good news, not bad news, because having found one, we can potentially do something about it. If we're ignorant of it, however, we probably can't fix it.

Security Paradigm 3 (Vulnerability Assessments)

Old Paradigm:
- Vulnerability Assessments (VAs) are done once every 1-5 years.
- Do it right once, and you can phone in future VAs.

New Paradigm:
- A VA is a dynamic, ongoing process that happens every day.
- Vulnerabilities (and our recognition of them) change rapidly with new technologies, different security personnel and adversaries, changing priorities, and improved understanding.

Security Paradigm 4 (Changing Vulnerabilities)

Old Paradigm:
- Vulnerabilities are relatively static.

New Paradigm:
- Vulnerabilities (or our understanding of them) change rapidly over time with new personnel, missions, adversaries, technologies, and insights.
- Fix one vulnerability, and you'll likely introduce multiple new ones or change the old ones.

Security Paradigm 5 (The Purpose of a Vulnerability Assessment)

Old Paradigm:
- A VA is a test you “pass”, or a “certification” you receive.

New Paradigm:
- A VA is for the purpose of improving security.
- “Passing” or “Failing” has little meaning.

Security Paradigm 6 (Minor Vulnerabilities)

Old Paradigm:
- Focus on the serious vulnerabilities (easiest to exploit, most likely to be exploited, worst consequence).
- Ignore minor ones.

New Paradigm:
- If the minor vulnerabilities are easy to fix or mitigate, do so because we might be wrong about them being minor, or there might be related serious vulnerabilities that we’ve overlooked.

Security Paradigm 7 (Audits)

Old Paradigm:
- We insure good security through security surveys and audits: reviewing the security policies, checking on how well security personnel know and follow the rules, and auditing compliance with regulations, guidelines, and policies.
- Focus on the existing security measures, plans, policies, and strategies, and on the currently deployed hardware and software.

New Paradigm:
- We improve security through VAs: finding vulnerabilities and suggesting countermeasures.
- We avoid being overly focused on Plans & Compliance.
- We don’t let the good guys and the current security posture define the security problem. The bad guys get to do this.

Security Paradigm 8 (Threats vs. Vulnerabilities)

Old Paradigm:

- Threats (who might attack, when, where, and with what resources and probabilities) are more important to understand than Vulnerabilities (weaknesses in security).

New Paradigm:
- Typically vulnerabilities trump threats: If you get the vulnerabilities right, you are probably ok if you get the threats wrong (which is easy to do because you are mostly speculating). But knowing the threats without understanding the vulnerabilities isn't very helpful.

Security Paradigm 9 (Threat Assessments vs. Vulnerability Assessments)

Old Paradigm:
- A Threat Assessment is a Vulnerability Assessment.

New Paradigm:
- Threat Assessments and Vulnerability Assessments are two different activities, both of which contribute to overall Risk Management (along with understanding assets, consequences if those assets are attacked, etc.).

Security Paradigm 10 (Features & Vulnerabilities)

Old Paradigm:
- Vulnerabilities exist independent of attacks.
- Facility features, structures, entry points, and missing security measures are vulnerabilities.

New Paradigm:
- Potential attacks are the vulnerabilities.
- Facility features, structures, entry points, and missing security measures are relevant only to the extent that they can play a role in an attack.
- A facility feature is not a vulnerability independent of the various attack scenarios that can utilize it.

Security Paradigm 11 (Formalism, Rigor, & Perspective for Vulnerability Assessments)

Old Paradigm:
- VAs should be formal, rigorous, objective, consistent, and reproducible.
- They should be from the perspective of the existing security deployment.

New Paradigm:

- VAs must be creative, subjective, intuitive, and done from the perspective of the bad guys.
- Formalistic (checklist) methods can still be used as a starting point, but we need to watch out for sham rigor, the fallacy of precision, and the fact that most vulnerabilities are critically dependent on local details and personnel.

Security Paradigm 12 (Vulnerability Assessment Personnel)

Old Paradigm:

- Only security experts trained in the formalism can participate in a Vulnerability Assessment.

New Paradigm:

- Clever, creative, hands-on, hacker and loophole finders familiar with the facility or organization should also be involved, even if not security professionals.

Security Paradigm 13 (Vulnerability Assessment Follow-up)

Old Paradigm:

- Vulnerability Assessors are finished once vulnerabilities or non-compliances are identified.

New Paradigm:

- (The same) Vulnerability Assessors are brought back after countermeasures are deployed to see if they are effective, and to determine what new vulnerabilities have been introduced as a result.

Security Paradigm 14 (Compliance)

Old Paradigm:

- Compliance gets us good security.

New Paradigm:

- Compliance—though it may be necessary and can be of value—often causes distractions, gets in the way of good security, or can even be wholly incompatible with it.
- Common sense and true security must trump security rules.
- If a given security rule truly makes sense for a given situation, enforce it. If, however, it is stupid or there is a better way, get rid of it, change it, or authorize an exception.

Note: Examples of Compliance Harming Security

- *All the paperwork, bureaucracy, data recording, & preparation for audits causes distractions and wastes resources.*
- *Creates wrong mindset: Security = Busy Work; Mindless rule-following; the Brass are responsible for security strategies & tactics, not me.*
- *An over-emphasis on fences (4.5 – 15 sec delay), entry points, and force-on-force attacks that leads to bad security.*
- *Background checks & polygraphs are the only recognized countermeasures to the Insider Threat.*
- *Security clearances require self-reporting of professional social or mental health counseling, thus discouraging such counseling.*
- *The rules require overly predictable guard patrols & shift changes.*
- *Little room for flexibility, individual initiative, hunches, resourcefulness, observational skills, or people skills among security personnel.*

Security Paradigm 15 (Confidence)

Old Paradigm:

• If we're in good compliance, we can feel fairly confident about our security.
• Security is almost guaranteed if everybody will do his/her job.

New Paradigm:

• Even if we're in compliance, we need to feel scared. Confidence is always over confidence.
• Security is difficult, and may not be fully possible.

Security Paradigm 16 (Special Cases)

Old Paradigm:

• Security Managers, Auditors, & Vulnerability Assessors frown on exemptions and special cases.

New Paradigm:

• Security Managers, Auditors, & Vulnerability Assessors encourage exemptions and special cases (and the independent, local reasoning they entail) when this improves acceptance, productivity, and security.

Security Paradigm 17 (Training Security Personnel)

Old Paradigm:

• Training for security personnel is mostly about making them understand security rules, policies, and procedures.
• Performance for security personnel is measured by how well they adhere to security rules, policies, and procedures

New Paradigm:
• Training for security personnel emphasizes "What if?" exercises (mental and field practice).
• Performance for security personnel is measured by how effectively and resourcefully they deal with day-to-day real-world security issues, and with "What if?" exercises.

Security Paradigm 18 (Security Awareness Training for Employees)

Old Paradigm:
• Security Awareness Training for general employees is for the purpose of threatening and intimidating them into compliance with the rules.

New Paradigm:
• Security Awareness Training seeks to motivate and educate general employees about security, and seeks their help.
• The emphasis is on what's in it for them, the organization, and the country.

Note: Effective Security Awareness Training
+ We train dogs. We educate, remind, encourage, motivate people.
+ It should promote, sell, & motivate good security by employees, contractors, and vendors.
+ Use examples. Show people how to do things, don't tell them what not to do.
+ Avoid the negative terms: Don't! Never! No!
+ What's in it for me?
+ Make connections to personal security: home computer security, burglary, identity theft, etc.
+ Refer to news stories about security breaches in other organizations and the consequences.
+ Have metrics for effectiveness of the training (and the security)
+ No dumb trivia questions on the quiz, e.g., "Who is head of Department S-47?"
+ Use people-oriented instructors, not bureaucrats, technocrats, burnouts, zombies, or dead wood.
+ Be entertaining, vivid, & positive, NOT threatening, boring, patronizing, or full of organizational charts, talking head videos with camera-challenged executives, references to federal CFRs, or self-serving fluff about HR, the security organization, senior managers, or the training department.
+ Comedy, Violence (verbal, physical, or implied), & Sexiness are memorable.
+ Less is more. Stick with the most important security issues.
+ Security Awareness posters should offer useful security tips & solutions, not

platitudes, mindlessness, insults, & threats. They should be designed so that they are not the target of ridicule, scorn or vandalism.

Security Paradigm 19 (People)

Old Paradigm:
- Process and Technology (in that order) are our main tools for providing security.

New Paradigm:
- People and Process (in that order) are our main tools (though Technology can help).

Security Paradigm 20 (Who Provides Security)

Old Paradigm:
- Trained security personnel provide security.
- Regular employees, contractors, & visitors are the enemies of good security.

New Paradigm:
- (The Insider Threat not withstanding) regular employees, contractors, visitors, and neighbors provide security, with help from trained security professionals.

Security Paradigm 21 (Security Experts)

Old Paradigm:
- Security managers and security consultants are the main experts on Security.

New Paradigm:
- Frontline security personnel and regular employees are the main experts on local Security.

Security Paradigm 22 (Hazing as a Metric)

Old Paradigm:
- Security is painful and must inconvenience and hassle employees, contractors, visitors, & customers if it is to be effective.
- Hassling is a metric for security effectiveness.

New Paradigm:

- Security must not interfere with productivity any more than necessary.
- Once Security becomes the enemy of productivity and employees, all is lost and the bad guys have partially won.
- Employee acceptance is one metric for effective Security.

Security Paradigm 23 (Insider Threat Mitigation)

Old Paradigm:
- Ignore or under-estimate the Insider Threat.
- Deploy minimal (or no) countermeasures.
- Don’t consider employee disgruntlement as an important Insider Threat issue, or something that can be mitigated.

New Paradigm:
- Use proactive countermeasures for the Insider Threat, including mitigation of employee disgruntlement.
- Recognize that domestic violence is often brought into the workplace.

Security Paradigm 24 (Due Diligence)

Old Paradigm:
- Due Diligence is doing the absolute minimum we can get away with, or what keeps us out of trouble with juries, or what similar facilities do, or what the rules, regulations, and guidelines specify, or what higher-ups and auditors make us do.

New Paradigm:
- Due Diligence is providing the best security we can.

Security Paradigm 25 (High Technology as a Silver Bullet)

Old Paradigm:
- Technology will solve some or all of my security problems.
- High tech = high security.

New Paradigm:
- Technology solves nothing (though it can be a useful tool).
- High-tech security devices, systems, and programs are often the easiest to defeat (with low-tech methods).

Security Paradigm 26 (The Past as a Guide to the Future)

Old Paradigm:
- Past security incidents (at my facility or others that are similar) are the best guide to future ones.

New Paradigm:
- Past security incidents may be a good place to start thinking about security, but they are not enough. Future catastrophic security incidents (especially terrorist attacks) often haven't occurred previously, plus each facility and security application is unique.

Security Paradigm 27 (Prevention vs. Mitigation, Recovery, and Resiliency)

Old Paradigm:
- Focus on Prevention
- Reactive security
- We prepare to fight the last war
- Scapegoating, fingerpointing, & over reaction after a serious security incident
- Panic-mode chasing after snake oil "solutions" and fads.

New Paradigm:
- Focus on Prevention, Mitigation, Recover, & Resilience
- Proactive security
- We prepare to fight the next war
- Learn from security incidents, with increased commitment after a serious incident, not retribution
- Do intelligent analysis and R&D for long-term solutions

Security Paradigm 28 (Layered Security)

Old Paradigm:
- Layered Security ("Security is Depth") is a mindlessly applied approach when security managers and organizations wish to avoid thinking carefully, critically, and creatively about security.
- "We have layered security" is the automatic knee-jerk response when any new vulnerabilities are discovered or there are security concerns or questions.

New Paradigm:
- Layered Security is implemented only after a careful analysis of the purpose of each layer, and how the various layers interact and support or interfere with each other.

* Having multiple layers is never used as an excuse to stop thinking, or avoid improving any one layer or the overall effectiveness of security.

Security Paradigm 29 (Perceptual Blindness)

Old Paradigm:
- The fact that people (including security guards, and seal & safeguards inspectors) are remarkably poor observers (and don't fully realize it) is not factored into security strategies.
- The power of misdirection, distraction, and sleight-of-hand is not appreciated.

New Paradigm:
- The lessons from 50 years of experiments by cognitive psychologists are taken to heart and the fact that people are lousy observers and aren't fully aware of it will be factored into any security plan.
- Countermeasures to perceptual blindness are developed and deployed, including the effective use of technology to overcome human perceptual and cognitive weaknesses.
- Awareness training about misdirection, distraction, and sleight-of-hand is common for security guards, inspectors, and other security professionals.

Security Paradigm 30 (Security Theater)

Old Paradigm:
- Security Theater (fake security for show) is often preferred over real security because it is easier and takes less thought.

New Paradigm:
- Security Theater is easy to spot using effective vulnerability assessments and/or by its characteristic attributes. (See, for example, RG Johnston and JS Warner, "Security Theater in Future Arms Control Regimes", Proceedings of the 51st INMM Meeting, Baltimore, MD, July 11-15, 2010.)

Security Paradigm 31 (Cognitive Dissonance)

Old Paradigm:
- Cognitive Dissonance—the mental tension between what we want to be true (we have good security) and what is likely to be true (there are problems)—is a major impediment to good security and security improvements.

New Paradigm:
- The signs of cognitive dissonance are recognized and the dangers are neutralized. These dangers include *self-justification* (self-serving rationalization and excuse making),

paralysis or *stagnation* (failure to confront serious problems or make necessary changes), *confirmation bias or motivated reasoning* (unduly dismissing ideas, arguments, evidence, or data that might call into question our current viewpoints, strong hopes, or past decisions).

Security Paradigm 32 (Security Culture & Climate)

Old Paradigm:
- The importance of having a healthy Security Culture is given lip service, but the concept is ill-defined and under-analyzed.

New Paradigm:
- Security Culture & Climate and their effects on security effectiveness are carefully considered, thoroughly analyzed, and fully appreciated.

Security Paradigm 33 (Security Standards)

Old Paradigm:
- Security Standards often institutionalize misleading terminology and sloppy practice.
- They tend not to be researched based, and frequently over simplify complex issues, and discourage careful, critical, and creative thinking about security issues.
- Security Standards are often manufacturer-dominated and used as weapons to exclude competitors and discourage alternate approaches (rather than encouraging compatibility and mutual cooperation).
- The “certifications” that get institutionalized are often meaningless.
- The standards can make security products and practices worse, and can be very difficult to modify or improve once in place.
- The claimed consensus is often illusionary.

New Paradigm:
- Security Standards avoid the problems of inflexibility, one-size-fits-all thinking, over simplification, and domination by special interests.
- Security efficacy, product quality, careful thinking, understanding, compatibility, and mutual cooperation are all enhanced by the Security Standard, not degraded.
- Sound terminology and best practices are encouraged.

Note: In my view, the recently instituted ISO Standard 17712 for mechanical seals (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41017) is a good, bad example of a severely flawed security standard that may even be dangerous.

Security Paradigm 34 (Control)

Old Paradigm:

- Control is Security.

New Paradigm:

- Control should not get confused with Security, and should be avoided to the extent practical.
- Privacy rights and civil liberties must be protected in any security program.
- We don’t win against terrorists by becoming like them, or violating our fundamental principles and values.