International Council For Industrial Security & Safety Management

Newsletter: June 2012

Let's professionalize the professionals...

http://www.wix.com/sbtyagi/iciss

In the past, CCTV systems were used principally for facility observation and surveillance. They were used for industrial application as well as production and process monitoring in high precision and highly vulnerable industrial processes. They were also used in airport and prison security.

Now CCTV Systems are also being used for controlling traffic flow to reduce congestion. With the development of new high-resolution CCTV camera systems with fast pan, tilt and zoom functionality and built-in auto-tracking capabilities, systems now add an extra dimension to road safety by providing fast identification of potentially hazardous situations and fast accident recognition.

CCTV systems designed for road and traffic surveillance have to contend with an exceptionally broad range of challenging situations - from monitoring high-speed intercity highway traffic to surveillance of crossroads and pedestrian crossings on relatively slow-moving urban roads. They also have to deal with varying visibility due to weather and changes in road lighting, which can vary from bright daylight to twilight to artificial lighting at night and within tunnels to even unlighted roads. Automatic character recognition is also becoming essential for identifying vehicle registration-number plates.

Thanks to advanced technologies almost every problem can be solved so surveillance systems can work more effectively through intelligent cameras and flexibly via network infrastructure. Everyday new algorithms are being written, new video analytics are being tried and tested and improved versions of CCTV software are being introduced making traffic monitoring and highway surveillance easy and effective.

Capt S B Tyagi
For ICISS

In a hierarchy, every employee tends to rise to his level of incompetence. Work is accomplished by those employees who have not reached their level of incompetence.

Choosing the Right Antiterrorism Crash Barrier

Security warning issued at major cities especially at Mumbai is not to be taken lightly. That the terrorists of ISI / Taliban brand have experience in such activities is proven if we recall the blast at Hotel Marriott in Pakistan. The Vehicle Borne Explosive Devises (VBED) have brought unprecedented death and devastation in past at **Federal Building' in Oklahoma City in** 1995 attack which killed 168 people.

In recent years, terrorist attacks using vehicle-borne bombs have become a worldwide threat. These attacks have migrated from targeting military bases to densely populated urban areas. **To protect critical facilities as well as human lives, security professionals need to completely assess potential vulnerabilities, which often is the most challenging task.** Multidisciplinary cooperation and technical integrations as well as multi-resilience protection systems are always the key features. In addition to active prevention of such man-made hazards in advance, passive perimeter security barriers provide an additional way to assure life and facility safety.

Framework to Select Barriers: The generic framework proposed here to select appropriate barrier types is illustrated in ***Figure 1***.

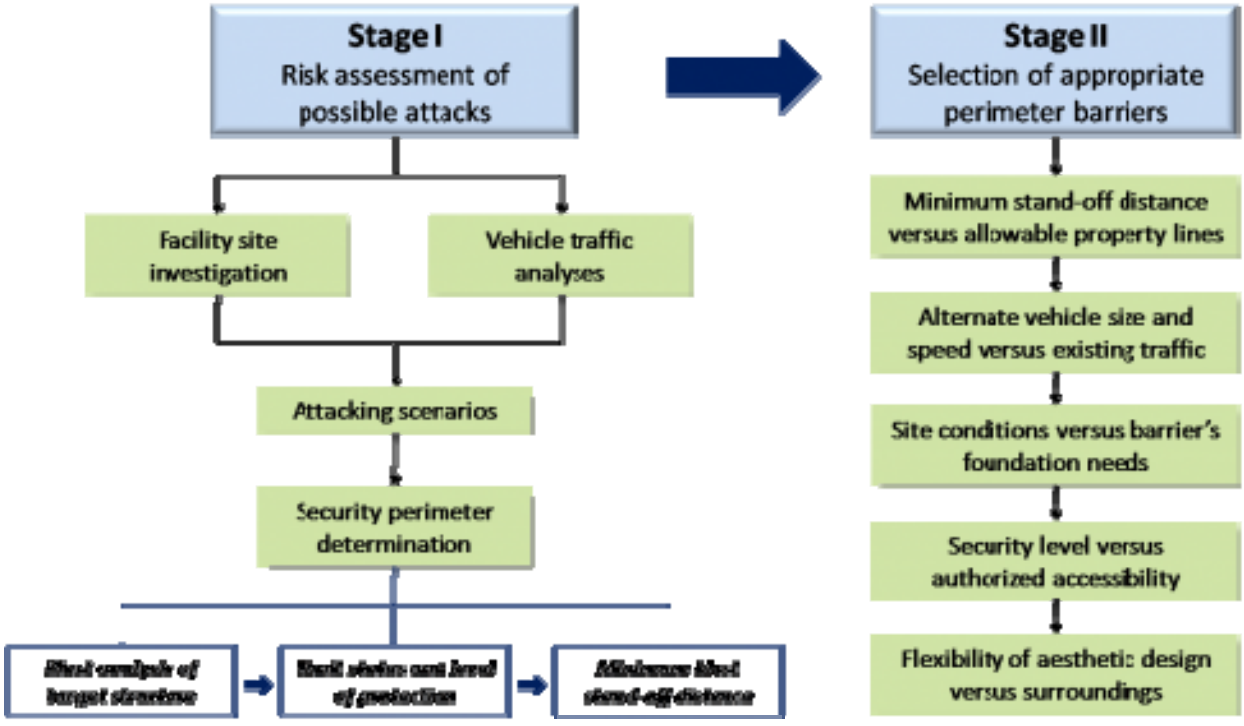


Figure 1 Generic Framework to Select Appropriate Barriers

Stage I: The first key stage is the risk assessment of possible attacks, which includes but is not limited to:

1) Facility site investigation to identify vulnerable spots surrounding the target.
2) Vehicle traffic analyses around the target, including two major components:

- ***Vehicle attacking scenarios:*** Performing traffic and vehicle motion studies to determine possible attacking vehicle types, traveling paths toward the target and maximum impact velocities along the paths **(Figure 2).**
- ***Authorized vehicle access:*** Clarifying client's needs and rearranging allowable paths and secured accessible points for authorized vehicles.

3) Determination of security perimeter.

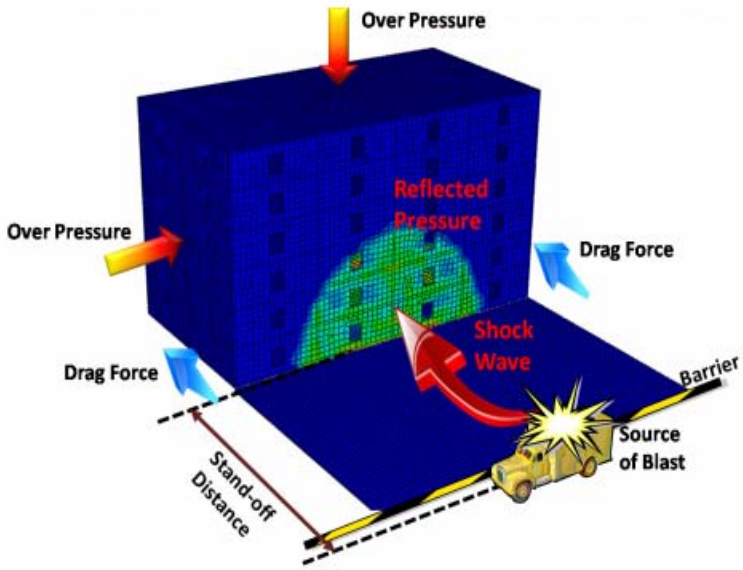


Figure 2 Explosive Blast Characteristics beside a Target Structure

Researchers have found that with certain explosive quantity, the blast overpressure and reflected pressure acting on the structure usually decays at a rate which is close to the reciprocal of cube of the stand-off distance. **Some past events have demonstrated this concept. The attack with about 4,000 lbs TNT-equivalent explosive at a 15-foot stand-off distance caused most of the 'Alfred P. Murrah Federal Building' in Oklahoma City to collapse.** This 1995 attack killed 168 people. **One year later, another attack with more than 20,000 lbs TNT equivalent at an about 80-foot stand-off distance only destroyed the front portion of the Khobar Towers in Saudi Arabia, killing 19 U.S. servicemen.** It is therefore crucial to assure the minimum stand-off distance between a target structure and an explosive-laden vehicle.

- ***Minimum stand-off distance:*** The minimum stand-off distance criterion can then be decided from the blast analyses results after owners choose what level of protection is adequate for their situation.

Stage II The second key stage is to select and implement the most appropriate physical perimeter barriers based on the outcome of Stage I. When selecting the perimeter barrier, the security professional needs to consider many key factors, including:

- Minimum stand-off distance versus allowable property lines;
- Possible maximum vehicle size and speed versus existing traffic;
- Site conditions versus barrier's foundation needs;
- Security level of protection versus accessibility for authorized people and vehicles;

- Flexibility of aesthetic design versus surroundings, especially in urban areas.

Figure 3 Structural Damage Limit State Definitions

New Barrier Technology Development To avoid deep excavations, some new concepts have been recently proposed, including shallow foundation mounted bollards, which typically employ large strong steel frames cast into a base concrete slab. If a vehicle crashes into it, the huge rigid impact forces will spread out over large areas, thereby limiting foundation damages. However the vast foundation work may create many other construction and cost issues.

Stopping the momentum of a terrorist vehicle requires changing its impact speed to zero forward velocity, without permitting significant penetration towards the target structure. Based on Newton's second law of motion, the vehicle's momentum (the vehicle's mass times velocity) can be successfully brought to rest at a zero velocity if a relatively low and constant deceleration force can be exerted for sufficient duration of time without failure, as shown in ***Figure 4***.

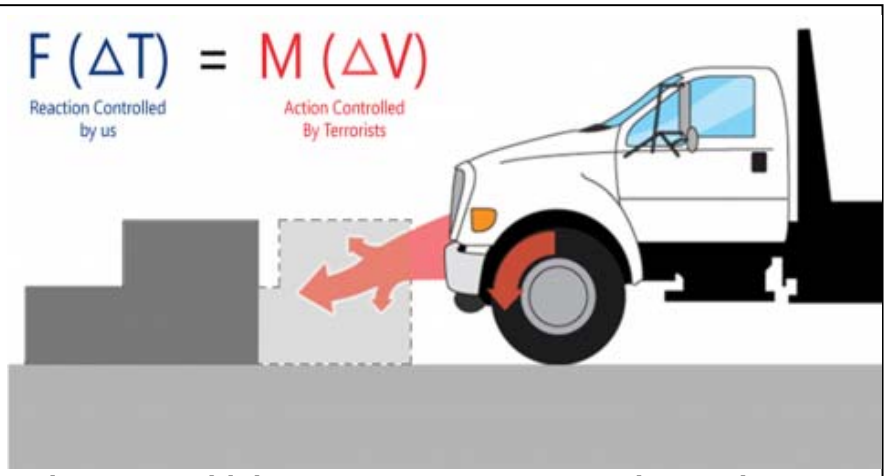


Figure 4: Vehicle Momentum versus Barrier Resistance

Precast reinforced concrete barriers containing energy absorbers become ideal because of the flexibility of both structural and geometric design, large stiffness and strength, compatibility to connections, and its secure nature against normal destructions. The barrier's decelerating energy dissipaters can be accurately set at any force and stroke required by analytic studies and crash validations. Such "calibrated" deceleration forces assure the deceleration of a vehicle to zero velocity outside the secured perimeter, while at the same time controlling the forces imposed on the foundation. The controlled shear force is transmitted to the foundation, either a sidewalk or deck, using mechanical interlocking at its underside as well as optional soil anchors that lock the existing diaphragm to the earth below. The proposed barrier technology eliminates any deep foundation needs by employing an effective load transfer mechanism with calibrated decelerating forces.

Numerical Crash Simulations and Prototype Crash Validations

Numerical simulations of a truck crashing into a physical barrier can be executed using advanced computer programs such as LS-DYNA3D, one state-of-the-art software in analyzing real-time dynamic behaviors considering actual geometry and material characteristics for both truck and barriers. It is always meaningful for the barrier developers to perform numerical simulations before directly jumping into field tests. High-tech expertise and powerful computer software as well as hardware make it possible to cover different barrier design options and many vehicle crash scenarios. The developers can then fine-tune the technical design based on results in the virtual world. The clients can also gain a good understanding of the barrier's performance under real attack predicted from the simulations **(Figure 5)**.

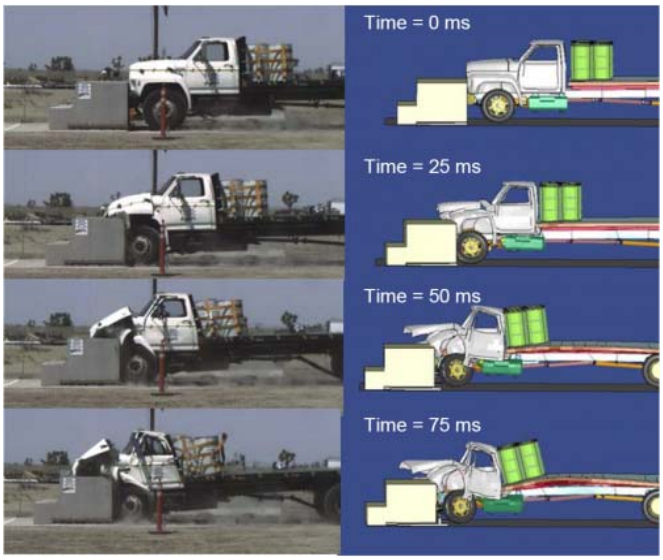


Figure 5 Field Crash Validation Compared with Computer-Based Numerical Simulations

Conclusions Because the science behind choosing the right protective barrier system directly relates to protecting human life and property, it must be a thorough process. To provide the most reliable and effective security solutions for clients, security professionals should utilize multi-disciplinary expertise to perform a systematic and comprehensive risk assessment, scientific structural analyses and barrier evaluations, and then recommend the right security barrier type and arrangement based off their client's particular needs.

As terrorism concerns underline the necessity of more and more anti-crash and anti-blast barriers throughout city landscapes, architects and designers have found many innovative ways to blend them into the urban environment based off their stakeholders' demands.

Nevertheless, security professionals will need to work ever more closely with architects and city planners in the design and implementation of vehicle control barriers to address more pressing functional requirements.

Van Herpen's Law: **The solving of the problem lies in finding the solvers.**

While buying the Security system that will help protect your family...

When considering which company will install the security system that will help protect your family for years to come, it is important you feel comfortable with your choice. After you have purchased, had the system installed and the technician has left, it is you who will live with the consequences. For this reason alone, it is very important to ask all of the right questions, so as to achieve the level of comfort you need.

The questions to ask are…

- How long has the company been in business under the same name?
- How many system installations has the company done?
- How many installations has the technician that will be installing your system performed?
- Are their technicians up to date on all the latest equipment? What type of training do they receive?
- Will you have a say on where they install the various components of your system?
- How will they wire your system? Will wires be visible?
- How many technicians will perform the installation? How long will it take?
- What brand of equipment do they install? Why?
- Will you own your system 100%? If not, who will?
- What happens when an alarm is tripped? What happens in the event of a false alarm?

7 Things You Should Know About Online Passwords

As online technology has advanced, so have hackers' techniques for getting into your accounts and stealing personal information. Hackers break into computers 2,244 times each day by figuring out weak usernames or passwords, according to University of Maryland data. If you're still using the same password you made up when you opened your first email account, you are setting yourself up to be a hacking victim. But don't worry; read on and learn how to set those 'Internet geniuses-gone-wrong' for failure by knowing the essentials about online passwords.

1. You need different passwords for each site

Since passwords are so hard to remember and you sometimes don't sign into a site for months, many people have one or two passwords they use for everything. This is an easy way for hackers to get access to your accounts. Hackers will infiltrate sites that aren't very secure and uncover the passwords used there. Then they run them on all the most popular sites; if you use the same password across the board, they can easily access several of your

accounts. By using a different one for each site you log into, you're not handing them your life if they figure out one password.

2. Longer passwords are harder to hack

It obviously takes less time to type in a five-character password than a 15-character one, but that also means it will take less time for an Internet burglar to figure out. Most of us probably don't have the interest or the determination to break into someone's account, so it's hard to imagine going through enough combinations to find out a five-letter password. Hackers have advanced programs, though, that allow their computers to go through hundreds of possibilities every minute. Each letter, number, or symbol you add to your passwords multiplies the time it takes to figure it out, hopefully frustrating the hacker enough that he gives up. A six-letter password that's all lower-case takes 10 minutes to hack while an eight-letter one takes four days.

3. You shouldn't use a word from the dictionary

A dictionary attack sounds like something an overworked English teacher would do, but it's actually a method of hacking passwords. Many hackers use automated password-guessers that go through the words in the dictionary to try to crack yours. If you've used any common words, there's a good chance that a person equipped with the right tools will be able to break into your account very quickly. By combining two or three dictionary words, you increase the amount of time it will take to guess it exponentially. By adding symbols and numbers in the middle of words, you protect yourself almost completely from a dictionary attack.

4. Humans tend to choose passwords with personal meanings

Because we as humans are so forgetful, our first instinct when choosing a password is to think of words that mean something to us personally. This makes our choices very predictable to hackers. Pet names, favorite sports teams, birthdays, and other personal bits of information are some of the most commonly used passwords, so if anyone knows even a little bit about you (or can find it on Facebook), you could be in trouble. Stay away from using your own name, names of people in your family, or any memorable dates. It should go without saying that you shouldn't be using "123456″ or "qwerty."

5. Passwords need to be changed regularly

Some offices and organizations require you to change your password every 90 or 180 days, and while it seems like a hassle, it's actually a smart practice to do with all your accounts. This is especially important to do with online banking sites or shopping sites where your credit card information might be stored. It's also necessary if you access any accounts on public or shared computers because your password may be stored without you knowing it and some hackers use programs that record your keystrokes. By regularly changing your password to something completely different, you lower the risk of any major damage being done if someone did manage to hack your account.

6. There are guidelines for creating strong ones

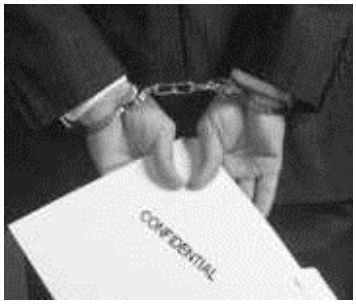
Now that you know you shouldn't use common words or your dog's name to access your online accounts, you might wonder what you should use instead. Most Internet security experts recommend having a password that's at least 8 characters long with a mix of capitalized and lower-case letters, numbers, and symbols. A common technique for avoiding easily guessed words is to put three unrelated words together and make up a short story that involves all three so you can remember it. You can also use the first letter of each word in your favorite line of a song or movie. Change out a couple letters for numbers or special characters, and your password should be too much trouble for a hacker to figure out.

7. Password managers can help you keep track of them all

Once you've updated all your passwords to long strings of letters and digits, you're probably going to forget one along the way. Security experts say it's a bad idea to write down a list of all your passwords and leave it on or near your computer because someone could easily steal it. The smartest alternative is to use a trusted password manager, which can be web-based technology, software you put on your computer, or a portable device. Password managers keep track of your various passwords and often protect against keystroke recording programs and look-alike sites that hackers use.

Business Intelligence

Business Intelligence is the process of optimizing your company's competitive advantage by the legal and ethical exploitation of all commercially pertinent information, whilst denying that same information to Competitors.



Many Business Intelligence Seminars and Services are on offer now-a-days aimed to show you how to maximize the information collection and analyze potential of your organization. These give you the tools and techniques you need, to exploit the wealth of open source intelligence data available in our industry. One has to learn how to transform Trade Shows from expensive corporate chores, into intelligence gathering goldmines, and how to use legally and ethically available information, to get an inside track on your competitor's latest development plans!

Of course, to fully maximize your advantage, you must also be able to restrict access to proprietary information which may be available to competitors, either through ethical information gathering or illegal (but all too common), industrial espionage. Many consultants and trainers are available to show you how your competitors may be using **illegal techniques** including 'bugs' and specialized computer technology, to access your information and steal your company secrets. They will then help you implement the appropriate defensive strategies to minimize any potential risk, or loss to your business.

Cyber-security: Indian to secure US teen site

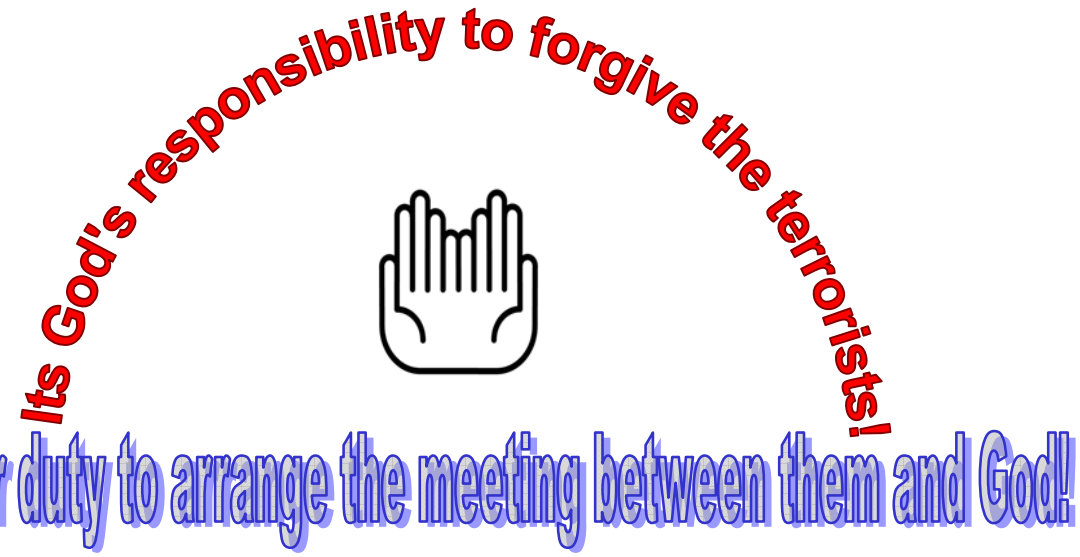
MySpace, US'S most popular social network site for teenagers, will soon have an Indian American online safety czar to deal with a growing menace of porn and sexual predators that has alarmed parents and law enforcement officials.

Hemanshu Nigam, a corporate Attorney of repute with Microsoft, has been handpicked to shore up the safety of a site that boasts of 70 million members and ranks second only to Yahoo in terms of page views. Nigam's induction to police the site, owned by Rupert Murdoch's Fox Interactive Media, comes close on the heels of a series of incidents in which sexual predators used personal information and profiles posted on MySpace to track down and molest teens.

"One in five kids online is sexually solicited. “Online predators know what they're doing. Do you?", reads one of the new public service ads now being put out by MySpace. Among recent incidents, a 22year-old man has been charged with raping a 15-year-old girl in Westford, Massachusetts. He had met the girl on MySpace. In Honolulu, a 29-year-old man assaulted a 15-year-old he met on the same site last month. Similar charges are faced by an older man in Abernathy, Texas.

Nigam, as the first-ever Chief Security Officer, will be the point-man for MySpace's safety, education, privacy and law enforcement program. A graduate from the Boston School of Law, Nigam has been a federal prosecutor with the US Department of Justice dealing with Internet child exploitation. He has also been an adviser to a Congressional commission on online 'child safety and to the White House on cyber-stalking.

"Hemanshu is a proven leader in online safety and security. We are fortunate to have him in MySpace, helping educate the public and protect our members' safety and privacy," said Chris De Wolfe, CEO of MySpace, a hip site that flaunts itself as the premier lifestyle portal for connection with friends and discovering popular culture. The "connected community" has been created by integrating web profiles, blogs, instant messaging, e-mail, musical streaming and videos, photo galleries and classified listings of events and groups.



In lighter veins

What does a computer system intruder look like?

16-29 year old male

Operates all times of the day.

Runs automated attack applications against 10's - 100's of hosts.

Uses vendor diagnostic applications to identify security weaknesses.

Keeps abreast of latest technical innovations.

Suggestions & feedback may be sent to us on e-mail: sbtyagi1958@gmail.com

P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address and we will move it out from our contact list, thank you!