ioMosaic®

Minimizing risk. Maximizing potential.®

Security Vulnerability Assessment (SVA) Revealed

An ioMosaic White Paper

Nature of Threats

Security threats can come from internal or external adversaries. Internal threats include disgruntled employees and/or contractors, or employees forced into cooperation by threat of extortion or violence. External sources include criminals, extremists or terrorists.

The most important objective of an adversary, next to successfully completing the mission, is not being detected. Detection usually results in a failed mission. Because the external adversaries may not need to enter your plant, there are few mitigation options for increasing the likelihood of detection prior to the attack. Furthermore, as a recent article in USA Today The Forum states, "Terrorists focus on simple means [to avoid detection]. They are going to use stuff that's available." We need to think like terrorists if we want to prevent an attack. "We're looking for this big, magical attack, and the terrorists are looking for stuff that's already in the environment."

Some chemical companies have already decided that protecting their assets from attack by armed combatants with military caliber weapons is the responsibility of government and local authorities. Furthermore, coupled with the terrorist's desire to be unobtrusive, such a scenario is not a high priority for prevention. Given that a chemical plant became the target, a more plausible scenario is the detonation of an SUV filled with ammonium nitrate and distillate fuel oil next to a storage tank. This only requires stuff that is already in the local environment.

Why is SVA Important?

While the likelihood of the terrorist threat is arguable, the consequences for a company aside from the obvious losses, could be quite harsh. Firstly, any significant emergency response effort due to a chemical plant attack would become a news media event. This guarantees high visibility. Secondly, if it were learned that the company had completely ignored the security risk and was unprepared, there would be a public outcry. [In addition, the industry has already been drawn into homeland security initiatives, whether it likes it or not]. So chemical and energy companies need to address the risk to some extent, but how much is the ongoing debate.

At the very least, understanding the security risk is a necessity. Many chemical companies have already screened their facilities and operations for security vulnerability potential and are conducing Security Vulnerability Analyses (SVAs) on the high priority concerns. Furthermore, there is no lack of ideas on how to assess the risks. Industry trade associations (e.g., American Chemical Council), professional societies (e.g., AIChE's Center for Chemical Process Safety) and the Justice Department have sponsored the development of SVA methodologies. The question is where do we go from here?

The Path Forward – Where Do We Go from Here?

A standard or code can be viewed as codified risk mitigation for a hazard (threat) that is pervasive throughout industry. For example, frequent boiler explosions in the past led to mechanical design codes for boilers and pressure vessels. More recently, the development of American Petroleum Institute Recommended Practice (API RP 752) for siting of buildings in process plants, addresses a common hazard to process plant control rooms, especially for plants designed when pneumatic controls were prevalent. The CCPS SVA Guidelines; Appendix A, addresses this aspect from the standpoint of the SVA methodology.

At the moment there is much passion and activity expended on SVA. What is missing is a practical industry consensus standard or recommended practice (similar to API RP 752) that allows companies to benchmark their individual security mitigation efforts. The development of such a recommended practice would allow pooling of the collective wisdom of CPI/HPI manufactures and consultants. It would also provide practical and consistent guidelines for addressing an industry wide potential problem. Such a standard would not limit individual companies from establishing internal practices that exceeded the established recommended practice if they so desire.

The focus should be on practical and implementable risk reduction based on “deter, detect, and delay” mechanisms incorporated into internal policies/procedures, perimeter security systems, and a rapid robust response. The recommended practice should also incorporate a risk-based assessment approach that puts terrorist attacks in context with other plant risks.

Finally, enhancement of post-incident response capabilities should be addressed. This would include a review of internal capabilities such as emergency isolation and shutdown, release mitigation options, communication, etc. Externally this might include a review of local emergency response coordination and resources leading to the development of a coordinated contingency plan for a high public impact event.

Issues

September 11, 2001, is to chemical plant security vulnerability what Bhopal, India was to plant process hazards vulnerability. Then, as now, awareness of the issue was strikingly revealed by a catastrophic event. In the case of process hazards vulnerability, government and industry initiatives were set in motion that eventually produces the OSHA Process Safety Management Rule (29CFR1910.119). It remains to be seen whether security vulnerability will be codified in a similar fashion. There are some indications that this may happen. The U.S. Department of Justice, Office of Justice Programs has already supported the development of the Chemical Facility Vulnerability Assessment Methodology (VAM), which was prepared by Sandia National Laboratories.

Chemical industry groups including the American Chemical Council (ACC) and The American Institute of Chemical Engineers Center for Chemical Process Safety (CCPS) have also responded with their own guidelines and methodologies for assessing treats of attack from internal and external activities. As of this writing there is no single consensus methodology for evaluating security vulnerability. In fact, there is hardly a consensus on how much effort needs to be expended on events that are highly unlikely for a given site, and that are all but impossible to control for some scenarios.

One of the questions is just how desirable a chemical facility to a terrorist is when considered in the context of all potential targets. Firstly, their prime objective is to cause mass casualties or massive disruption because they are expending resources over a considerable time period. As the 9/11 pre-attack activities demonstrate, it took many months of planning to orchestrate and implement that incident. The target must have a high probability of achieving the prime objective, once attacked. Targets that would meet this criterion include dams, nuclear power stations, energy pipelines, and rail systems (especially toxic chemical shipments).

In many cases targeting chemical plants may not achieve the same level of assurance for success. As we know from risk assessment studies and experience, the occurrence of a toxic or flammable chemical release does not always have a catastrophic consequence, especially for the offsite public. A review and interpretation of the Chemical Safety Board incident database provides some additional perspective. Of 167 reactive chemical incidents, there are about 40 that had a public impact of some kind (Table 1).

The breakdown by severity of impact is given below:

Table 1: Breakdown of Impact

Severity of Impact	Number of Incidents	Percentage of Incidents
Public Evacuation Only	13	32.5
Injury to Public	5	12.5
Public Fatality	1	2.5
Other (Sheltered in place)	21	52.5
TOTAL	**40**	**100**

These incidents were not screened for size of release and are not all worst-case scenarios. But the numbers do show that public impact events are less than half (40/167) and suggest that mass casually events are a small percentage of public impact events. Perhaps the main insight derived

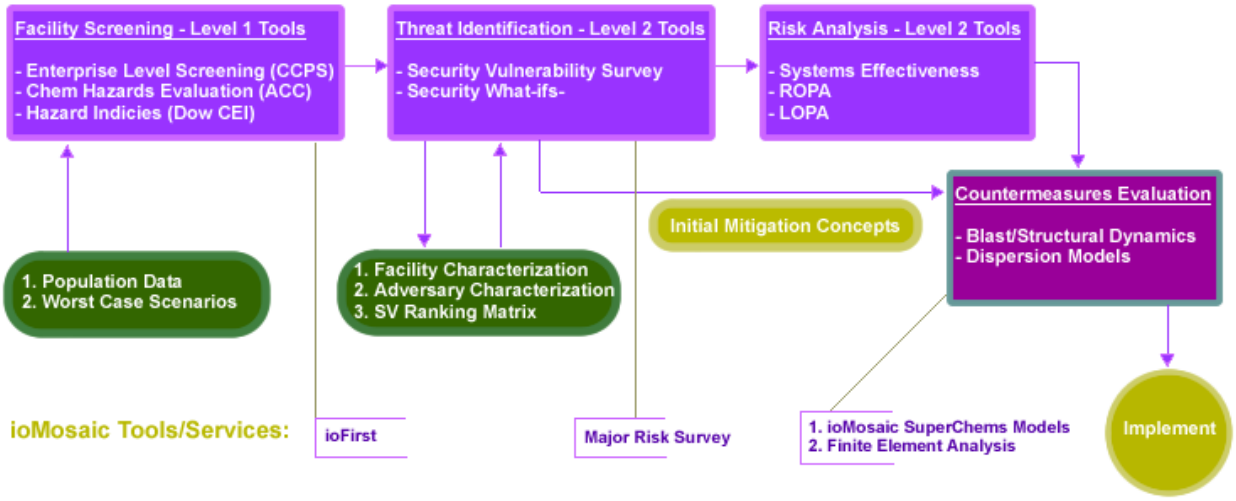
from this data set is that only worst-case scenarios need to be considered in security vulnerability assessment, because smaller events will not produce the desired impact.

Another factor is the degree of access. Energy or chemical pipelines and rail lines and storage yards are less secure and much easier to attack without notice. Protecting such assets is also difficult. A 60 Minutes™ documentary noted that rebels in Colombia blowup the same petroleum pipeline about every two weeks, even though it is expected.

What Does Security Vulnerability Assessment (SVA) Involve?

The chemical security vulnerability assessment is basically a review of a companies assets for handling, storing, and processing hazardous materials from the perspective of an individual or group intent on causing a catastrophic event with large-scale injury/fatality or supply disruption impacts. It considers possible scenarios by looking at inventories or production steps involving hazardous material, potential pathways of attack, and existing security countermeasure or ring of protection. The scenarios are priority ranked using a system of risk-based factors, which estimate (usually qualitatively) the frequency and consequence of each scenario. High priority scenarios are subjected to further assessment to consider appropriate mitigation options (countermeasures). In some cases (controversial or expensive fixes), more quantitative risk assessment tools may be employed to help reach a decision.

Figure 1: Security & Vulnerability Assessment Methodology



Get Started - Security Vulnerability Screening

For some guidance, it is useful to again return to the period following Bhopal, to consider how some large multi-product, multi-facility chemical companies were approaching risk assessment. At that time, a tiered or layered risk analysis concept (Ref.1) was applied, because the effort involved a full quantitative risk assessment (QRA) was resource (personnel and time) intensive and not warranted in many cases. This tiered concept is illustrated in Reference 1 and gives examples of the tools that are appropriate for each tier. This same approach makes a lot of sense for the current situation with SVA and is supported by the American Chemistry Council (Ref. 2).

The first step involves security vulnerability (SV) screening using Tier 1 tools. Tools that are available that fall into this category include:

- Chemical Hazards Evaluation (Ref. 2)
- CCPS Security Vulnerability Enterprise Screening Tool (Ref. 3)

These tools are not complex and are intended to facilitate the prioritizing of facilities processing or handling chemicals, prior to conducting a Security Vulnerability Analysis (SVA).

Table 2 provides a comparison of the factors that are considered in the screening. While not a tool per se, Step 1.0 of the VAM is also included for completeness. The CCPS screening tool is basically an index method that incorporates “difficulty of attack” and target “attractiveness. It builds on the RMP worst-case scenarios by incorporating the results of those consequence analyses. However, for non-RMP scenarios, the CCPS consequence evaluation is less quantitative. For these scenarios, other tools like the DOW Chemical Exposure Index (CEI), or Facility Initial Risk Screening Tool (ioFIRST), available from ioMosaic Corporation can be utilized. The latter computerized screening tool incorporated simplified hazard models for toxic and flammable materials, which are sufficiently robust for screening purposes. The SV screening produces a list of sites or facilities that is divided into several priority tiers (e.g., 1 to 4 for CCPS tool).

Table 2: Comparison of the Factors Considered in Screening

ACC General Approach	CCPS Enterprise Level Screening	VAM Step 1 Screening
1.0 Chemical Hazard Evaluation: 1. How likely is a chemical release, and 2. How harmful would it be?	1. Relative Difficulty of Attack factor considers ease of access and complexity of logistical support 2. Relative Severity factor considers population density within the radius of impact of RMP "worst case" scenario.	1. Specify undesirable events 2. Evaluate consequences of undesirable events
4.0 Physical Factors 1. Size of Container? 2. Where is it located? 3. What surrounds the plant site, and at what distance?	1. Relative Severity factor is based on worst case release 2. Relative Attractiveness factor considers proximity to national landmarks, critical infrastructure, etc. 3. Addressed by Relative Severity factor population density aspect	Considers: 1. Number of people affected 2. Recognized importance, history/symbolism 3. Accessibility
	Non-RMP covered facilities or chemicals with potential offsite impact: 1. Determine Relative Severity factor base on engineering estimate of hazard distance and impacted population	If on-site inventory is less than threshold quantities (TQs) for covered chemicals under 40 CFR 69.130, then a VA is unlikely to be needed to help protect against unacceptable off-site consequences.
	When utilizing off-site consequences is inappropriate (e.g., small quantities of chemical warfare chemicals, FBI list chemicals) 1. Computation (by spread sheet) of a Material Factor based on toxicity, explosivity, reactivity an storage method.	Second question is whether the loss of a facility would result in a significant national impact (e.g., sole source for a chemical vital to national defense industries).

Table 3: Summary of the Features of Three (3) Public Domain Methodologies

Element	ACC SSG	CCPS SVA	Sandia VAM
Screening	Step 1: Chemical Hazard Evaluation: • How likely is a chemical release, and • How harmful would it be?	Enterprise Level Screening • Relative Difficulty of Attack factor considers ease of access and complexity of logistical support • Relative Severity factor considers population density within the radius of impact of RMP "worst case" scenario.	1.0 Screening • Specify undesired events • Evaluate consequences of Undesired Events
Threat Identification Assessment	Step 2: Process Hazard Analysis Step 3: Consequence Assessment Step 4: Physical Factors Assessment	Step 2: Facility Characterization: • Assets/hazard ID, Consequence analysis Attractiveness analysis, Layers of protection review Step 3: Threats Assessment: • Adversary ID/ characterization	3.0 Planning: • Characterize facility • Derive severity levels • Threat Assessment 4.0 Site Survey
Risk Analysis		Step 4: Vulnerability Analysis • Target classification or Site security review and scenario development • Risk analysis	5.0 Analysis • Systems effectiveness analysis • Risk Analysis
Mitigation	Step 5: Mitigation Assessment	Step 5: Identify Countermeasures	6.0 Risk Reduction
LESS	⇦ Formalized Methodology ⇨		MORE

The next step is to subject the high priority facilities to a more detailed vulnerability analysis that considers specific attack scenarios and existing countermeasures or layers of protection. The techniques and the sequence of use in a VA are discussed next.

Vulnerability Assessment

A summary of the features of three public domain methodologies is presented in Table 3. The three approaches presented are:

1. Site Security Guidelines (SSG), a product of American Chemical Council (ACC) et. al.
2. CCPSR Security Vulnerability Analysis (SVA) Methodology
3. National Institute of Justice Chemical Facility Vulnerability Assessment Methodology (VAM) developed by Sandia.

Table 4: Level Two Tools

Methodology Element	Tool	Description
Threat Identification	SV Risk Survey	Experienced-based approach that employs a team to conduct a facility survey of potential security vulnerabilities
	SV What-if	Generic What-if checklist with questions specifically tailored to SV threats and existing protection layers
	Process Hazards Analysis al. a. SVA	Incorporation of SV into PHA techniques such as HAZOP etc.
Risk Analysis	Layers of Protection Analysis	LOPA is a simplified risk analysis tool which assigns probability reduction credits to various engineered and procedural independent protection layers (IPLs)
	Rings of Protection Analysis	ROPA is similar to LOPA, but is a more qualitative approach used by security specialists for considering protection layers

As can be seen, they have many risk assessment elements in common with variability in the sequence of when they are used. The three methodologies also vary from left to right in terms of the degree of formality and documentation involved. There was an attempt to make VAM a regulated standard (S.1602), but this appears to be less likely due to the change in the political landscape in Congress (Ref . 8).

By distilling the essences of these approaches, what emerges is a generic SVA methodology shown in Figure 1 that incorporates the layered risk assessment concepts discusses above. Some applicable Level 1 and Level 2 tools are shown in the major activity boxes. Specific tools that are available from ioMosaic Corporation are shown as flags.

Level 1 Tools have been already described. Some Level 2 Tools that may be employed are shown in Table 4.

Risk Management

Most companies have the tools and where with all to assess their vulnerabilities. The big question is what do you do to address the potential threat?

As mentioned, there are two groupings of adversaries, namely, insiders and outsiders. Risk mitigation controls need to be implemented to deal with both. Some of these will deal with the frequency component of risk and others address consequence mitigation.

1. Internal threats: Mitigation mostly involves administrative controls such as:
   - Employee hiring screening
   - Contractor screening
   - Perimeter security procedures
   - Behavior observation program
   - Inventory reduction
   - Emergency response planning
2. External threats: Mitigation involves more engineered controls:
   - Inventory reduction
   - Relocation of storage
   - Obscuring storage, installing decoy tanks
   - Improvements to physical perimeter systems (double fence line, lighting, motion sensor alarms, video cameras, Jersey barriers, etc.)
   - Pre-planning/coordination with local emergency response agencies.

Another way of look at security is using the Rings of Protection concept. This is analogous to the Layers of Protection concept used in process safety management. For example, the following ring structure could be considered:

Ring 1: Internal policies and practices

Ring 2: Parameter security systems and procedures

Ring 3: Storage inventory management and siting

Ring 4: Policing by local authorities

As Table 5 shows, the degree of company control, effectiveness, and cost can vary a lot, especially at the outer rings. In Step 11 of the Sandia VAM, the value of protection for common vulnerabilities is presented. Outer ring protections can help provide early detection to some threats, but inner ring

protections often address more threats and places delay and response features closer to a target. Furthermore, delaying an adversary is one of the important features of a good protection system because it impedes progress (which may also make the target less desirable) and allows time to mobilize an effective response.

Table 5: The Degree of Company Control, Effectiveness and Cost

Ring of Protection	Threat Addressed	Mitigation Concepts	Ability of Company to Control
1	Internal due to sabotage by third party or employee	Internal policies and practices: • Sign-in policies • Badge checks, receptionist • New employee and contractor screening • Behavior observation program	Entirely within plant's control. Generally low cost for implementation.
2	External due to unauthorized entry to plant site	Parameter security systems: • Double fence line • Trenches • Lighting • Motion sensor alarms • TV cameras	Entirely within plant's control. Low to medium cost for implementation.
3	External due to munitions delivered from outside the fence	Storage inventory management and siting: • Reduced inventory • Relocated storage • Obscure visibility of storage • Install shielding or berms	Mostly within plant's sphere of control but fixes may not be practical nor completely effective and can be costly. Risk/benefit analysis needed for deciding action
4	External due to munitions delivered from outside the fence	Increased policing by local law enforcement and/or improved ER coordination	Actions can be influenced by plant, but not totally controlled. Cost to plant may be negotiable.

The value of deterministic risk assessment is limited in security vulnerability analyses, particularly for the frequency dimension of risk. Placing probability/frequency estimates on some of the initial events involved an attack scenario is pure speculation. The initial vulnerability screening values are generally sufficient to identify the higher risk situations. A methodology like Layers of Protection Analysis (LOPA) could be used to evaluate the relative risk reduction benefit of mitigation options or rings of protection (ROP). One also has to ask how many rings are enough? If two good rings provide an expected frequency of < 10-6/yr., what more is needed?

Companies have found it more useful to apply quantification techniques to the consequence aspects of risk.

Explosion and vapor dispersion hazard models, like those in ioMosaic's SuperChems software, can be utilized to evaluate pre- and post mitigation concepts. Blast modeling of worst-case bomb threats coupled with structural dynamics can provide guidance on setting access exclusion zones and possibly hardening of the target structure. Dispersion models can be used to evaluate the effectiveness of post-release mitigation concepts (i.e., covers on liquid pools) as presented on the CCPS Book Guidelines for Post-release Vapor Mitigation.

Case Study

The following case study illustrates how hazard modeling can assist in the quantification of the impact of threats and the development of mitigation concepts.

Consider the following scenario where a terrorist loads an explosive on the back of a truck and parks the vehicle in close proximity to a storage tank containing a toxic chemical. The vehicle is parked on the side of the road outside the plant fence line. The storage tank is located about 200 ft. from the road.

For illustrative purposes, let us assume that the vehicle contains the equivalent of about 1200 lbs. of TNT. The overpressure caused by the explosion of 1200 lbs of TNT is shown in Table 6. The damage resulting from overpressure is shown in Table 7.

Table 6: Overpressure Profile From A 1200 16. TNT Explosive Blast

Overpressure (psi)	Distance (ft.)
1	950
3	450
5	330
7	270
9	240
12	200
15	180

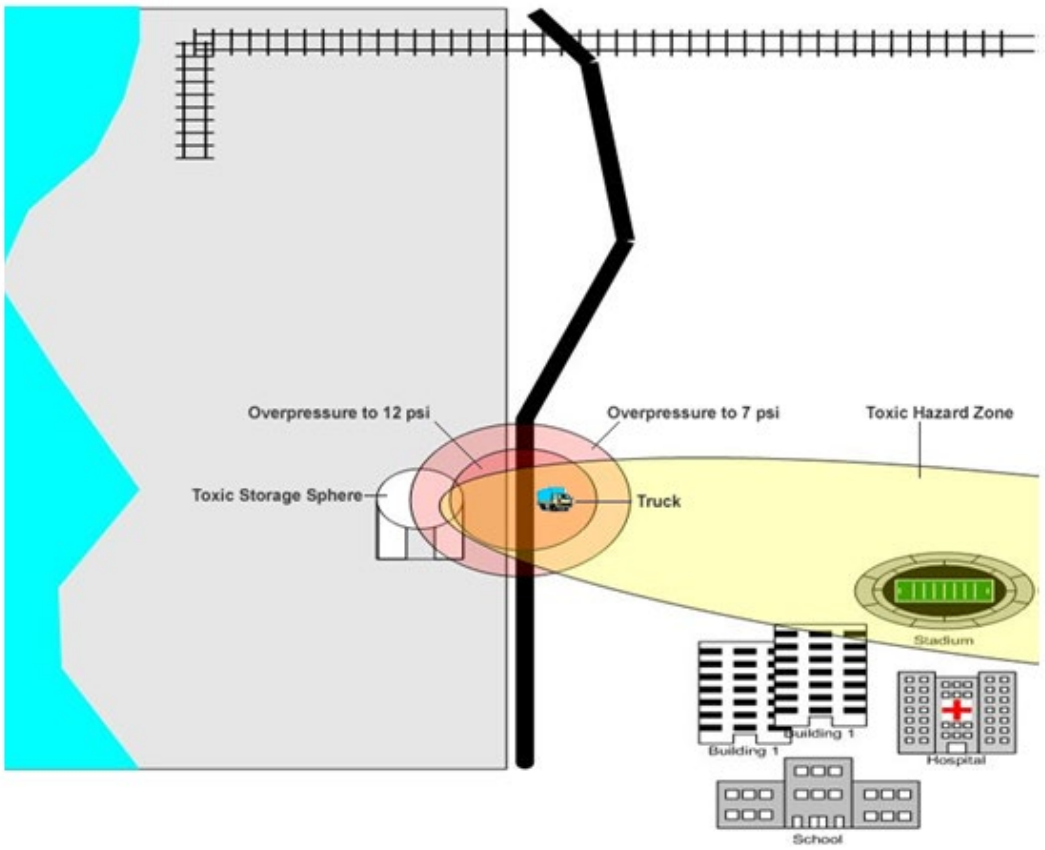
Table 7: Consequences Of Selected Overpressure (based on [Clancy, 1972] And [Glasstone and Dolan, 1997])

Peak Side-on Overpressure (psi)	Consequences
5	Most buildings completely destroyed, except for concrete reinforced (or masonry) shear wall buildings
3	Total destruction of unreinforced masonry wall buildings. Typical design criteria for many blast-resistant buildings. Rupture of oil storage tanks.
1	Upper limit of blast-resistance for most buildings of ordinary construction. Partial collapse of unreinforced concrete or masonry walls. Typical houses made uninhabitable. Persons knocked down by blastwave.
0.15	Typical lower limit for glass window breakage.

Based on these rough calculations, the overpressure will cause the storage tank to rupture. This will result in a toxic release. Based on dispersion calculations, the release will go a distance of 5 miles to the ERPG-2 level of concern. The scenario therefore has a severe offsite impact, and the security needs for mitigating this scenario needs be explored in greater detail.

On further analysis of the scenario using more detailed explosion models and structural dynamics, it was found that the tank would not fail given at a distance more than 150 ft. from the blast epicenter. Based on these results, the facility ownership decided to install greater perimeter security including electronic surveillance to monitor vehicular activity on the road.

Figure 2: Overpressure Profile From A 1200 16. TNT Explosive Blast



Upcoming Standards

NFPA is developing two new codes pertaining to security. The NFPA 730 (Premises Security Code) covers the overall security program for the protection of premises, people, property, and information specific to a particular occupancy. The NFPA 731 is a standard for the installation of electronic security systems.

References

1. Stickles, P., Ozog, H., Long, M., Major Risk Survey, AIChE National Meeting, Orlando, 1990
2. Security Vulnerability Enterprise Screening Tool, Center for Chemical Process Safety,
3. Site Security Guidelines for the U.S. Chemical Industry, American Chemistry Council (ACC), Chlorine Institute (Ci), Synthetic Organic Chemical Manufacturers Association (SOGMA), P.6
4. CCPS SVA Book
5. The Forum, Terrorists focus on simple means, USA TODAY, December 3, 2002
6. Johnson, J., Locking Down U.S. Industry, C & E News, October 28, 2002
7. Guidelines for Post release Mitigation Technology in the Chemical Industry, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 1997
8. Washington Update, Passage of Chemical Security Act Seems Unlikely, CEP November 2002

Additional Resources

1. R.Peter Stickles, 2006
2. Henry Ozog, 2006
3. Sanjeev Mohindra, 2006