

RISK DECISION-MAKING FOR CHEMICAL PROCESS SECURITY

David A. Moore, PE, CSP[1] and Lawrence M. Stanton, CPP, CFE[2]
[1]President and CEO, AcuTech Consulting Group, Chemetica, Inc., 88 Kearny Street, Suite 1630, San Francisco, CA 94108; dmoore@acutech-consulting.com
[2]Senior Security Consultant, AcuTech Consulting Group, Chemetica, Inc., 88 Kearny Street, Suite 1630, San Francisco, CA 94108; lstanton@acutech-consulting.com

INTRODUCTION

In the preceding years to the terrorist attacks in the United States of September 11th, 2001, the chemical industry focused its process safety activities on accidental release risks. Rarely, if ever, was consideration given to the risk of intentional release, or beyond that, the differences in the nature of such a release. This was most likely due to a perception that these risks were managed adequately, and that the threat of a terrorist attack, particularly on U.S. chemical manufacturing facilities or the supporting transportation system, was remote. Even within government law enforcement and intelligence circles, there was apparently a widely held assumption that terrorist objectives did not involve mass destruction attacks. Today, however, both the government and we in industry know better. The pendulum has swung, and with this new terrorism paradigm comes the knowledge that there is now real cause for concern regarding such a threat.

The new *terrorism paradigm* — that mass-destruction attacks are possible, obviously creates a new *risk paradigm* for the chemical sector. That is our assets can be targeted, both as a venue for a mass destruction attack, and as a vector for a mass destruction attack. This possibility must therefore inform our security planning and decision-making. Reasoned and informed security decision-making where chemicals and chemical facilities are concerned requires a new kind of risk judgment made against a fuzzy set of threats; all with a sense of urgency not previously experienced in accidental risk management.

Security Vulnerability Assessment methods such as the American Institute of Chemical Engineers' "Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites"[1], have been published to help structure the analysis process. These "SVA" processes are designed and employed to identify potential point targets of terrorism, and to classify these potential targets in broad terms. By doing so, we can begin the process of deciding how best to address vulnerability, when and where it is found.

[1]Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites, American Institute of Chemical Engineers, August 2002.

As a complement to these analytical approaches, companies need to develop risk acceptance criteria and decision tools to guide SVA teams in their counter-measures selection. For it is only by using the results of an analytical process to make the best, most informed possible decisions, that the analytical process yields value. Accordingly, it is in the interests of the industry itself to analyze its post-9/11 vulnerabilities as rationally as possible, and to establish rules for risk-assessment judgments that are consistent, reasonable, and complete.

Without a clear set of rules for making risk assessment judgments, security design against different threats may well be inconsistent, incomplete or inadequate, thereby negating the value of the invested effort.

The problem we face is very challenging. What do we do about this new risk and how do we know we have reduced the risk to an acceptable level? Public fear of terrorist attack on a chemical facility or its supporting transportation infrastructure is quite high, and there is an intuitive understanding that risk acceptance relative to acts of malfeasance may need to be different than has been the case in preventing accidental events.

This paper will address concepts such as the development of a threat-basis in support of the decision making process and addressing vulnerability in the context of a company standard. In the absence of government intervention in determining security standards or in determining acceptable risk criteria, industry is left with justifying their own decisions, and reasoned, transparent baselines for decision-making such as these criteria will be critical to the SVA process and its acceptance to the public and to government regulators.

THREAT-BASIS FOR SECURITY DECISION-MAKING

A threat-basis is nothing more complicated than a theoretical adversary, or what is often referred to in the security profession as the "assumed threat". In order to evaluate risk as it is posed by acts of malfeasance, it is essential to attain a baseline understanding of the potential assumed threat. There are several key things you need to know about the adversary, or, in the absence of knowledge, things you will have to assume. These are his motives, capabilities, and intent. Against this, you need to balance an understanding of the infrastructure you seek to protect. Most especially, you need to understand the way(s) in which your facility and/or materials could help the assumed threat achieve his aims. The problem in doing so is that the possibilities are, literally, endless. People are indeed as varied in motivation and capabilities as imaginable, and so our best option is to develop a hypothetical assumed threat who poses *a credible threat*. For that we assume he will correctly identify the most lucrative target(s) you are charged with protecting, and adopt his capabilities and intents as they pertain to those most lucrative targets as your upper end threat basis.

How does a typical manufacturing firm go about developing this hypothetical threat? How does that company match this theoretical attacker with a potential target? Doing so requires a couple of skills which are not often found in one person, or even one profession. Insight into human possibilities, motives and so on will rarely be

coupled with the necessary expertise in chemical process hazards. So far, these skill-sets are not inherent in any single profession. Accordingly, a partnership is called for, a cooperative effort among process safety experts, dangerous goods transportation experts, engineers, management and security professionals. Within a company, within a community, a region, or an industry, the need to bring these disciplines together is manifest. By doing so, the manufacturing firm enables itself to develop a reasonable, transparent threat-basis against which they can design security counter-measures.

The process of skills integration is now well underway in the United States. It is unusual today to attend a safety conference where there are no security professionals in the audience or on the dais, and the reverse is also true. The cooperation among these different professions has begun to yield superior results, far better than could have been realized by any one professional community.

One clear manifestation of this cooperative effort has been the development of the American Institute of Chemical Engineers (AIChE), Center for Chemical Process Safety (CCPS), "Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites".

That methodology describes an approach to security assessments which starts by making the assumptions described above. In the CCPS methodology, this technique is described as an "Asset-Based" Vulnerability Assessment. It is, in fact, nothing more than a threat-based design platform, wherein the company determines the upper limit threat against which they will assess risk and design countermeasures.

In the context of security, a threat basis is simply an established (and therefore consistent) description of the potential adversary who will, in theory, conduct the malicious act. The methodology seeks to overcome several basic challenges in applying safety evaluative methods to security by establishing the security equivalent of a risk-base.

By establishing a threat base, we have the first factor of the vulnerability equation, the *assumed threat*, the security equivalent of the *failure* in a safety analysis.

The establishment of a threat base yields additional benefits:

- It provides a reasoned upper limit for expenditures, on a consistent and transparent basis, thereby defusing some of the harshest potential criticism of industry efforts.
- It establishes a range of security events which require external assets to address, whether they are industry or community consortiums, or government/industry partnerships, or both.
- It sets out a rule for deciding on countermeasures, a rule that can be shown to outside stakeholders, and if appropriate, discussed and modified.
- It eliminates one of the more frustrating arguments encountered by security practitioners when seeking project funds — "we can't protect against everything, so why should we protect against anything?"

Figure 1 shows the theoretical adversary sets that a company has chosen as its threat. As you can see, the company has described four hypothetical adversaries, and assigned a class name to each of them. These hypothetical assumed threats serve as the basis for

Application of Security Functionality Requirements to the Assessed Risk Level (Ranking) of US Chemical Facilities			
	Tier 1 Facility	Tier 2 Facility	Tier 3 or 4 Facility
Level X Security			
Level A Security			
Level B Security			
Level C Security			
Level Definitions:	Level X	Provide security which is effective in deterring, detecting and delaying a carefully planned, highly destructive attack, to which the attackers have allocated significant resources.	
	Level A	Provide security that is effective in deterring, detecting and delaying a planned attack by a small team of trained individuals with limited access to resources.	
	Level B	Provide security that is effective in deterring, detecting and delaying a relatively unplanned attack, undertaken by an untrained person with very limited resources.	
	Level C	Provide security that is effective in deterring, detecting and delaying criminal acts, improving where necessary over previous practices.	
	Site Security System Functionality Requirement		
	Functionality not required and/or not achievable without outside assistance		

Figure 1. Threat-basis matrix

assessing vulnerability during the SVA, and then for development of appropriate countermeasures. Note that these classes of assumed threat are keyed to the Enterprise Screen tool used in the chemical sector to prioritize facilities within a given company for evaluation and security enhancement (Tier 1 — high consequence, attractive target, etc). Thus, the

determination as to what extent the company will go to protect a potential target is uniform across the company's locations and uniform across time.

The horizontal axis — Tiers 1 through 4, describe the site, or in the case of a transportation system, the route or mode. These "Tiers" describe a rough estimate of a site's potential to produce a consequence of attack that is reasonably consistent with terrorist objectives, and the "attractiveness" of the target from the point of view of a terrorist. In this case, "attractiveness" is used as a surrogate for a safety analyst's frequency of occurrence factor. These calculations — consequence and attractiveness, are described further below.

In viewing Figure 1, it is helpful to bear in mind the ways in which a chemical facility can be used to realize terrorist goals;

1. As a venue for a mass destruction attack (for example, by attacking a plant and releasing a massive quantity of an inhalation toxin);
2. As a vector for a mass destruction attack (for example, by diverting a large quantity of a pyrophoric chemical, then using it as an improvised explosive device against a "soft" target;
3. As a key node in an economic (national defense/public health) attack (for example, by destroying a key piece of production equipment that will have a massive cascade effect on industry)

And so we have a threat basis, and by understanding the three ways a chemical target can be used, we have a design basis. The next step is to correctly identify the potential targets and why they are targets, so we can design and implement security able to prevent these events, and to do so within the context of the potential assumed threat, the terrorist. That step, certainly the most challenging, is accomplished through the execution of an SVA.

ENTERPRISE SCREENING

The establishment of a threat-basis is one of the two key steps taken in advance of conducting an SVA. The second is the performance of an Enterprise Screen. Such a screen is simply a "first look", which has as its objective, the relative ranking of a company's facilities so as to facilitate prioritization. As a side benefit, the screen also identifies key vulnerabilities in terms of consequences and attractiveness, the second and third evaluative factors.

The Enterprise Screen looks at entire sites as a single entity. Thus, evaluation is usually applied to the single most lucrative potential target, though, in some cases, the cumulative value of several potential point targets may be considered. The screen looks at two issues, Attractiveness and Consequences.

ATTRACTIVENESS

This is a subjective value used as a surrogate for frequency. Since it is impossible to know the "frequency" of attack on a given specific facility or point target, another value must be

used in substitution. Where the safety professional or engineer can got to the literature and determine (scientifically) what the expected rate of failure for a given type of flange in a given set of conditions is, there is no such literature, or history, available to determine an equivalent probability for a terrorist attack. There are, however, factors available to us that can be used to determine how attractive a given piece of infrastructure, process or material is to the hypothetical assumed threat who is serving as our threat basis. These factors are well-known in military circles, as they constitute the basis for targeting doctrine, used by the US Military to select point to be attacked in times of conflict. While not quantitative, these factors are things that can be reasonably assumed, and so a valuable qualitative assessment of a given potential target's attractiveness is possible.

Attractiveness factors are derived from the threat basis. These factors are discussed in greater detail in the SVA section below.

CONSEQUENCE OF ATTACK

The consequence of attack calculation is better understood within the chemical industry. For the most part, this portion of the assessment is derived from existing data, addressing the potential consequences of an accidental release. In general terms, extensive refinement of existing calculations regarding release is not required; after all, a cloud of ammonia does not behave differently if it has been released accidentally or deliberately.

However, some factors do need to be considered when "translating" accident scenarios into a terrorist event application. First and foremost, the evaluator needs to consider the response/containment/remediation capability in the new (terrorism) context. Depending on how a facility is laid out, it may be necessary to assume substantial degradation of response capabilities as a part of the attack. This, of course, may impact the consequence assessment. It may also be necessary to consider releases not reasonably envisioned in accident scenarios, for instance, the simultaneous runaway reaction of 5 storage tanks, as opposed to an accident scenario, where there it is never assumed more than two vessels would begin to polymerize at one time.

Note the similarities between the evaluation of consequence and the earlier evaluation of attractiveness. This is due to the fact that the same circumstances that indicate possible high casualties will also tend to make that facility an attractive target for terrorist attack. Thus, certain factors, such as the potential for producing large numbers of casualties, are in effect double weighted in the enterprise screening process.

SECURITY VULNERABILITY ASSESSMENT AND SECURITY MANAGEMENT PRINCIPLES

The next component in the decision process is the Security Vulnerability Assessment. Owner/Operators should ensure the security of facilities and the protection of the public, the environment, workers, and the continuity of the business through the management of security risks. The basic premise is that security risks should be managed in a risk-based, performance-oriented management process.

The foundation of the security management approach is the need to identify and analyze security threats and vulnerabilities, and to evaluate the adequacy of the countermeasures provided to mitigate the threats. Security Vulnerability Assessment is a management tool that can be used to assist in accomplishing this task, and to help the owner/operator in making decisions on the need for and value of enhancements.

The need for security enhancements will be determined partly by factors such as the threat, the degree of vulnerability, the possible consequences of an incident, and the attractiveness of the asset to adversaries. In the case of terrorist threats, higher risk sites are those that have critical importance, are attractive targets to the adversary, have a high level of consequences, and where the level of vulnerability and threat is high.

SVAs are not a quantitative risk assessment, but are performed qualitatively using the best judgment of the SVA Team. The expected outcome is a qualitative determination of risk to provide a sound basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures.[2]

A basic premise is that all security risks cannot be completely prevented. The security objectives are to employ four basic strategies to manage the risk including Deter, Detect, Delay, and Respond. Appropriate strategies for managing security can vary widely depending on the circumstances including the type of facility and the threats faced by the facility. Therefore, the use of an SVA as a means of identifying, analyzing, and reducing vulnerabilities is the most sensible approach. The specific situations must be evaluated individually by local management using best judgment of applicable practices. Appropriate security risk management decisions must be made commensurate with the risks. This flexible approach recognizes that there isn't a uniform way to "do" security in the chemical process industry, and that resources are best prioritized to first address high risk situations.

SVA METHODOLOGIES

There are several SVA techniques and methods available to the industry, all of which share common elements. Ultimately, it is the responsibility of the owner/operator to choose the SVA method and depth of analysis and documentation that best meets the needs of his specific situation. Differences in location, type of operation, and on-site type and quantity of hazardous substances all play a role in determining the level of SVA and the approach taken. Independent of the SVA method used, all generally-accepted techniques include the following:

- Characterize the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure, and the consequences if they are damaged or stolen
- Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each adversary

[2]Ibid, AIChE.

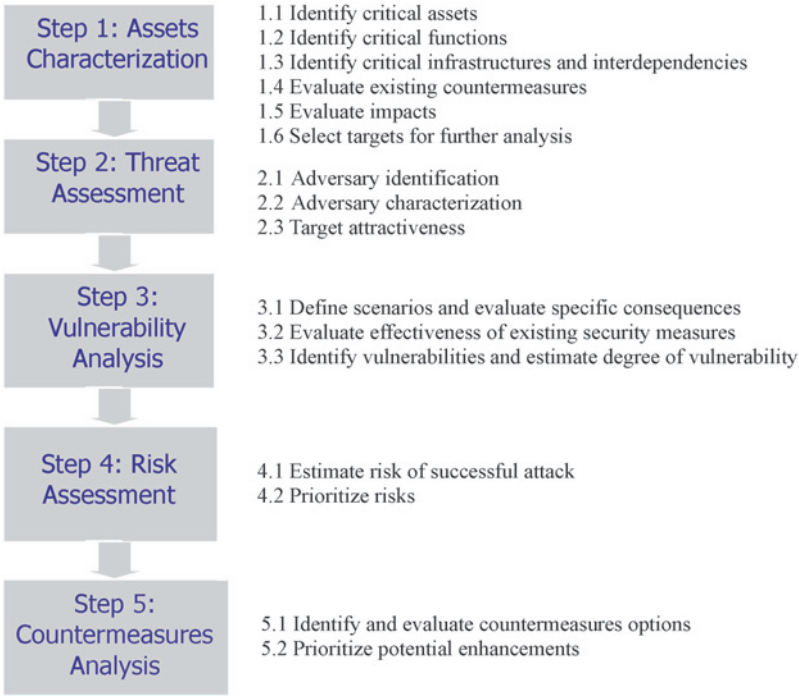

Figure 2. API/NPRA security vulnerability assessment methodology

- Identify potential security vulnerabilities that threaten the system's service or integrity
- Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the consequences of an event if it were to occur
- Rank the risk of the event occurring and, if high risk, make recommendations for lowering the risk
- Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses) and re-assess risk

One approach to conducting an SVA is shown in Figure 2. This methodology was published by the American Petroleum Institute and the National Petrochemical and Refiners Association in their guidelines "Security Vulnerability Assessment for the Petroleum and Petrochemical Industries", May, 2003.[3]

[3]"Security Vulnerability Assessment for the Petroleum and Petrochemical Industries", American Petroleum Institute, May, 2003.

Intentional Release Risk is a function of:	Accidental Release Risk is a function of:
• Consequences of a successful attack against an asset and • Likelihood of a successful attack against an asset.	• Consequences of an accidental event and • Likelihood of the occurrence of the event.
Likelihood is a function of: • the Attractiveness to the adversary of the asset, • the capabilities of the attacker, and • The degree of Vulnerability of the asset.	Likelihood is a function of: • The probability of an event cascading from initiating event to the consequences of interest and the frequency of the events over a given period.

Figure 3. Intentional release vs. accidental release risk definitions

DEFINING THE RISK TO BE MANAGED

For the purposes of an SVA, the definition of risk is shown in Figure 3 and 4. The risk that is being analyzed for the SVA is defined as an expression of the likelihood that a defined threat will target and successfully attack a specific security vulnerability of a particular target or combination of targets to cause a given set of consequences. This is contrasted with the usual accidental risk definitions in Figure 3.

OVERVIEW OF AN SVA METHODOLOGY

The SVA process is a risk-based and performance-based methodology. The user can choose different means of accomplishing the general SVA method so long as the end result meets the same performance criteria. The API methodology is very similar to the previously-cited American Institute of Chemical Engineers SVA and to several others in widespread use. The overall 5-step approach of the API/NPRA SVA methodology is described as follows:

Step 1: Asset characterization

The asset characterization includes analyzing information that describes the technical details of facility assets to support the analysis, identifying the potential critical assets, identifying the hazards and consequences of concern for the facility and its surroundings and supporting infrastructure, and identifying existing layers of protection. Essentially, this step identifies the assets (people, facilities, information, reputation, business) of value, analyzes why it is of value and identifies its importance, determines the interaction

Consequences	The potential impacts of the event
Likelihood	Likelihood which is a function of the chance of being targeted for attack, and the conditional chance of mounting a successful attack (both planning and executing) given the threat and existing security measures. This is a function of three variables below.
Threat	Threat, which is a function of the adversary existence, intent, motivation, capabilities, and known patterns of potential adversaries. Different adversaries may pose different threats to various assets within a given facility.
Vulnerability	Any weakness that can be exploited by an adversary to gain access and damage or steal an asset or disrupt a critical function. This is a variable that indicates the likelihood of a successful attack given the intent to attack an asset.
Target Attractiveness	Target Attractiveness, which is a surrogate measure for likelihood of attack. This factor is a composite estimate of the perceived value of a target to the adversary and their degree of interest in attacking the target.

Figure 4. API/NPRA SVA methodology SVA risk variables[4]

of the assets with other neighboring facilities, suppliers, or customers or other economic interdependencies.

Assumptions are made on the worst credible security event consequences to etermine the impacts. The estimate of severity of the consequences is one of the four risk factors.

Step 2: Threat assessment

The intentional release risk includes possible attacks by outsiders or insiders, or a combination of the two adversaries. It may be perpetrated by a number of different adversaries with varying intents, motivations, weapons, tactics, and capabilities. These issues need to be sorted out in a threat assessment, which is, in effect, a risk-based assessment that forms the basis of the design basis threat assumption the facility designs and operates to.

The selection of the threats should include reasonable local, regional, or national intelligence information, where available. This step also includes determining the target attractiveness of each asset from each adversary's perspective.

A responsible company has to give thought to the possible threats and attempt to organize the many combinations and permutations into a threat matrix. Key to this matrix is the first variable — what is the target? Is the company a direct target or is it affected by a terrorist attack? From a pure risk management standpoint, companies need to be prepared for both contingencies, not only for the possibility of direct physical or

[4]Ibid, AIChE.

cyber attack to their facilities. This shows the multi-faceted aspects of the problem, and the need for industry, community and government cooperation to address the problem.

For example, there is a major difference in the protection set required if the assumed threat is an armed attack by a small band of terrorists who use force to enter the main entrance way, vs. a single insider who misuses their access to the process control system to cause a release from the same asset. Which threats are credible and to what extent is the threat potential?

Threat is an important factor in the determination of risk. Prior to September 11th, 2001, for example, many of the other factors in the risk equation were present, but the threat was considered to be too low to be credible. It is the increased appreciation of threat that prompts us to now take action. Properly done, the threat assessment forms the basis of the process security management strategy for the facility.

The threat definition results in a determination of the design basis threat for the facility. The threat assessment results in a 'fixed' and 'variable' design basis threat. The fixed threat forms the basis for the design and is the baseline threat estimate. The variable design basis threat assessment is an estimate of the change in threat levels given certain possible future conditions. The U. S. Homeland Security Advisory System (HSAS) is an example of a national effort to help define varying threat levels. Facilities are urged to take actions given increased threat levels, so these factors need to be considered in the threat assessment.

The concept of fixed and variable design basis threats is useful for making decisions on facility design and operation. If the threat to insiders is considered significant, countermeasures designed to limit those risks are imperative. The fixed threat may determine the need for background screening, limiting the span of control of individuals, strong supervision, monitoring of activities, audits, surveillance, password controls, and other measures. In fact, after determining and appreciating that the insider threat potential threat is significant, the facility may be designed or redesigned to avoid use of a type of operation, substitute chemicals, or other measures to minimize this potential. If other conditions change, the threat may increase. For example, if there are a large number of visitors such as during a turnaround or in the event of specific threat information or a terrorist attack in the United States, increased threat levels may change or add to the baseline countermeasures.

Threat to a particular asset varies with several factors including the degree of interest that an adversary may have in the asset, as well as the degree of impact possible if the asset was attacked, disabled, copied, compromised, or stolen. For this reason, the threat assessment includes a step whereby each asset is analyzed from the perspective of each potential adversary to determine the degree of attractiveness of the asset to the adversary. Attractiveness is therefore another factor in the determination of risk.

Step 3: Vulnerability analysis

The vulnerability analysis includes the relative pairing of each target asset and threat to identify potential vulnerabilities related to process security events. This involves the identification of existing countermeasures and their level of effectiveness in reducing

those vulnerabilities. The degree of vulnerability of each valued asset and threat pairing is evaluated by the formulation of security-related scenarios or by an asset protection basis. If certain criteria are met such as higher consequence and attractiveness ranking values, then it may be useful to apply a scenario-based approach to conduct the Vulnerability Analysis. This approach option is very similar to the PHA techniques employed to analyze accidental releases. It includes the assignment of risk rankings to the security-related scenarios developed.

Vulnerability is important to understand as it helps to determination how adversaries may target and execute crimes. Vulnerabilities are ubiquitous, so simply understanding vulnerabilities is not sufficient to make a risk determination. Other factors such as threat, consequence, and attractiveness are required for a more complete risk appreciation.

Step 4: Risk assessment

The risk assessment determines the relative degree of risk to the facility in terms of the expected effect on each critical asset as a function of consequence and probability of occurrence. Using the assets identified during Step 1 (Asset Characterization), the risks are prioritized based on the likelihood of a successful attack which is a function of the threats assessed under Step 2 and the degree of vulnerability identified under Step 3.

Risk assessment is only possible when there is some frame of reference. Since the events in question are extremely rate events, it is necessary to 1) use surrogate factors such as attractiveness and threat to determine the likelihood of interest of attack of any particular asset, and 2) use vulnerability as a measure of the likelihood of a successful attack given the desire to attack. Then the analyst can use performance criteria to set risk goals. Each scenario is evaluated against those goals. For example, such criteria as the following may be set to determine unacceptable risk:

Security criteria:

- No unauthorized person can easily cross the outer perimeter without delay or detection;
- Any intruder is detected within 10 seconds of breaching the perimeter barrier;
- Any intruder is interdicted within 5 minutes of breaching the perimeter barrier;
- Any person entering the secured zone is authorized to be there;
- Authorization is comprised of invitation and verification;
- No unauthorized vehicle shall be allowed within 500 feet of a critical asset.

These criteria are used as binary risk goals, i.e., if the existing situation fails these tests, then additional countermeasures are required.

Step 5: Countermeasures analysis

Based on the vulnerabilities identified and the risk that the layers of protection are breached, appropriate enhancements to the security countermeasures may be recommended. Countermeasure options will be identified to further reduce vulnerability at the facility. These include improved countermeasures that follow the process security doctrines of

deter, detect, delay, respond, mitigate and possibly prevent. Some of the factors to be considered are:

- Reduced probability of successful attack and degree of risk reduction by the options
- Reliability and maintainability of the options
- Capabilities and effectiveness of mitigation options
- Costs of mitigation options
- Feasibility of the options

The countermeasure options should be re-ranked to evaluate effectiveness, and prioritized to assist management decision making for implementing security program enhancements. The recommendations should be included in an SVA report that can be used to communicate the results of the SVA to management for appropriate action.

SUMMARY

The problem we face is clear. What do we do about this new risk and how do we know we have reduced the risk to an acceptable level?

What we do about this new risk is what we did about the old risks; we bring our collective wit to bear, we work together, we share insight, knowledge, best practices, and lessons learned. We develop a reasoned, systematic, documented and transparent approach to assessing where we are vulnerable to terrorist attack. We determine, as companies, as industries, as nations, what our risk tolerance is. Then we put into place the measures necessary to reduce, as much as we reasonably can, the vulnerabilities we've identified.

There is no great mystery here. The processes and programs we've developed over the years in order to address safety concerns are adaptable to today's security challenges, but the must be adapted. We as an industry must work together to ensure that adaptation is appropriately done and appropriately applied. We as a profession must ensure that we enlist the cooperation of the security profession in this effort.

The development of a threat-basis in support of the decision making process is the first step; conduct of an enterprise screen is the second. Performance of an SVA is the third, and development and installation of appropriate security countermeasures, including where applicable, Inherently Safer Technology, is the point of all that precedes it. Following such an approach will enable a company to justify their decisions, showing how they used reasoned, transparent baselines for decision-making.