ELSEVIER

Journal of Hazardous Materials 115 (2004) 175–180

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

The new risk paradigm for chemical process security and safety

David A. Moore[1]

AcuTech Consulting Group, Chemetica, Inc., 1948 Sutter Street, San Francisco, CA 94115, USA

Available online 28 September 2004

Abstract

The world of safety and security in the chemical process industries has certainly changed since 11 September, but the biggest challenges may be yet to come. This paper will explain that there is a new risk management paradigm for chemical security, discuss the differences in interpreting this risk versus accidental risk, and identify the challenges we can anticipate will occur in the future on this issue. Companies need to be ready to manage the new chemical security responsibilities and to exceed the expectations of the public and regulators. This paper will outline the challenge and a suggested course of action.

1. A new awareness of deliberate release potential

Prior to 11 September, chemical process risk management activities focused on accidental release risks, and excluded most considerations of intentional releases. This was most likely due to a perception that these risks were managed adequately, and that the threat of a terrorist attack or other intentionally caused event, particularly on U.S. chemical manufacturing facilities or transportation systems, was remote.

The pendulum has dramatically swung the other direction, and now there is a real concern for this new threat, as well as a sense of urgency for protection against these types of potential events. The risk of another major attack in the U.S. is seen today by most terrorism experts as not a question of 'if', but when. Violent acts by extremist environmental groups or disgruntled employees have occurred in various cases. Extrapolating this concern broadly to the chemical process industry, there is an extraordinary dilemma in play. The current perceived threat has created a confusing atmosphere and pressures on industry to make immediate changes. This has created a need to analyze this threat and to make necessary changes to reduce the risk. Most of the changes are unplanned, potentially expensive step-changes in security. Hopefully, we would not be forced to make sacrifices in our accidental risk efforts in light of the urgency for security improvements.

In fact, deliberate release risk should be managed by many of the same or similar strategies as accidental release risk. Traditional security countermeasures, such as physical security features and cyber security measures, must integrate with safety strategies to result in a single process risk management strategy.

2. Risk paradigm

Depending on the degree of exposure potential of the company or the public from an intentional release, the attractiveness of a target, and the ease of attack, companies may face entirely different risks than the facilities were designed to manage. It could require a very different mode of operation and security than is currently being employed.

At this juncture, most companies handling hazardous materials would admit that considerations of terrorist attack were not given much thought initially. There are trillions of dollars of infrastructure in the United States that has not been designed against extreme acts of violence. But they are struggling to understand the risk and do the right thing right away. Many companies have already done some form of threat assessment and security vulnerability assessment, and have

E-mail address: dmoore@acutech-consulting.com.

[1] Present address: AcuTech Consulting Group, Chemetica, Inc., 88 Kearny Street, Suite 1630, San Francisco, CA 94108, USA. Tel.: +1 415 772 5972; fax: +1 415 772 9044.

0304-3894/$ – see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2004.08.017

upgraded some physical and operational security measures. Still there is much work to be done.

The bigger problem is facing the new quandary of this risk – what do we do about it and how do we know we have reduced the risk to an acceptable level? Public fear of this risk is extraordinary, and so risk acceptance could likely be altogether different. The risk decisions we have made over the years that seemed adequate for accidental risk may not be adequate for intentional risk.

Worse than this, the sky seems to be the limit for what may go wrong and what industry may have to do to prevent or protect against these threats. Sorting out the real risks from the possible threats is going to be a major undertaking, and there is much uncertainty at this point on how to accomplish such a risk assessment and how to cope with this threat.

3. Security vulnerability assessment and security management principles

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 (SVA) 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 degree of 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 to 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 riskincluding 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 facing the facility. As a result, it is difficult to prescribe security measures that apply to all facilities in all industries, but instead it is suggested to use SVA as a means of identifying, analyzing, and reducing vulnerabilities. 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 approach to security in the chemical process industry, and that resources are best applied to mitigate high risk situations primarily.

This is a new area of process risk management, and much has to be done to further understand the potential, determine analysis methods, develop supporting guidance, and educate managers and engineers on how to manage the issue, to name a few activities required. Also, we have to come to grips with the determination of risk, and to decide on which threats are worthy of further analysis and change to our processes and the way we manage them.

4. 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 that best meets the needs of his specific location. Differences in geographic location, type of operations, and on-site quantities of hazardous substances all play a role in determining the level of SVA and the approach taken. Independent of the SVA method used, all 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.
- 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 a SVA is shown in Fig. 1. This methodology was published by the American Petroleum Institute and the National Petrochemical and Refiners Association in their guidelines "Security Vulnerability Assessment

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

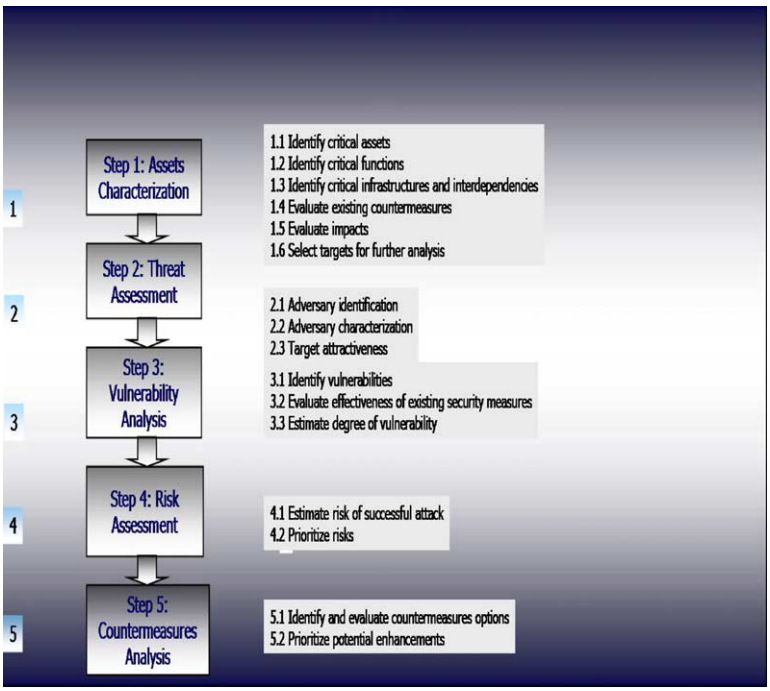

Fig. 1. API/NPRA security vulnerability assessment methodology.

Intentional Release vs. Accidental Release Risk Definitions	
Intentional Release Risk is a function of: • Consequences of a successful attack against an asset and • Likelihood of a successful attack against an asset.	Accidental Release Risk is a function of: • 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 degree of Threat posed by the adversary, 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.

Fig. 2. Intentional release vs. accidental release risk definitions.

for the Petroleum and Petrochemical Industries", May 2003.[3]

5. Defining the risk to be managed

For the purposes of an SVA, the definition of risk is shown in Fig. 2. 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. The risk variables are defined as shown in Fig. 3.

6. Overview of a 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

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

API/NPRA SVA Methodology SVA Risk Variables[3]	
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.

Fig. 3. API/NPRA SVA methodology SVA risk variables ("Security Vulnerability Assessment for the Petroleum and Petrochemical Industries", AIChE).

meets the same performance criteria. The overall five-step approach of the API/NPRA SVA methodology is described as follows.

6.1. 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 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 determine the impacts. The estimate of severity of the consequences is one of the four risk factors.

6.2. 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 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, versus 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 11 September 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 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, disables, 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.

6.3. 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.

6.4. 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 (Section 6.1), 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 rare 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 s of breaching the perimeter barrier.
- Any intruder is interdicted within 5 min 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 ft 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.

6.5. 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.
- 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.

7. Conclusions

Expectations for security have greatly changed since 11 September. The problem is we are not all prepared to deal with the threat. There is a new risk paradigm that requires a different form of analysis than accidental risk assessment methods. The overall strategy to address the issue involves three basic steps. The first step is to accept that the threat exists. The second step is to analyze the threats and vulnerabilities. The third step is to define a security management system that meets the criteria. All the while, industry faces a dilemma of elevated levels of perceived threat to the industry and the need to make risk decisions under extreme uncertainty in the short term.