ELSEVIER

Journal of Hazardous Materials 130 (2006) 107–121

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

Application of the API/NPRA SVA methodology to transportation security issues☆

David A. Moore*

AcuTech Consulting Group, Chemetica Inc., 88 Kearny Street, Suite 1630, San Francisco, CA 94108, USA

Available online 19 September 2005

Abstract

Security vulnerability analysis (SVA) is becoming more prevalent as the issue of chemical process security is of greater concern. The American Petroleum Institute (API) and the National Petrochemical and Refiner's Association (NPRA) have developed a guideline for conducting SVAs of petroleum and petrochemical facilities in May 2003. In 2004, the same organizations enhanced the guidelines by adding the ability to evaluate transportation security risks (pipeline, truck, and rail).

The importance of including transportation and value chain security in addition to fixed facility security in a SVA is that these issues may be critically important to understanding the total risk of the operation. Most of the SVAs done using the API/NPRA SVA and other SVA methods were centered on the fixed facility and the operations within the plant fence. Transportation interfaces alone are normally studied as a part of the facility SVA, and the entire transportation route impacts and value chain disruption are not commonly considered. Particularly from a national, regional, or local infrastructure analysis standpoint, understanding the interdependencies is critical to the risk assessment.

Transportation risks may include weaponization of the asset by direct attack en route, sabotage, or a Trojan Horse style attack into a facility. The risks differ in the level of access control and the degree of public exposures, as well as the dynamic nature of the assets.

The public exposures along the transportation route need to be carefully considered. Risks may be mitigated by one of many strategies including internment, staging, prioritization, conscription, or prohibition, as well as by administrative security measures and technology for monitoring and isolating the assets.

This paper illustrates how these risks can be analyzed by the API/NPRA SVA methodology. Examples are given of a pipeline operation, and other examples are found in the guidelines.

Keywords: Security vulnerability analysis; American Petroleum Institute; Transportation

1. Introduction

The security risks associated with the transportation of assets is a complex issue but a necessary one to analyze in a security vulnerability analysis. Given that most SVAs have focused on the fixed facility assets rather than the entire value chain of the operation, this is a ripe area for security evaluation. The American Petroleum Institute, recognizing the need for a methodology for evaluation of transportation risks, recently expanded their SVA guidelines to include consideration of this risk.

The American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) developed the first edition of this Security vulnerability assessment methodology available to the petroleum and petrochemical industry in 2003. The information contained in the document was developed in co-operation with government and industry, and is intended to help refiners, petrochemical manufacturers, and other segments of the petroleum and petrochemical industry maintain and strengthen security of their personnel, facilities, and operations, and to thereby enhance the security of the nation's infrastructure.

API decided that it would be beneficial to use a single methodology for both facility and transportation risks.

☆ 7th Annual Symposium, Mary Kay O'Connor Process Safety Center "Beyond Regulatory Compliance: Making Safety Second Nature" Reed Arena, Texas A&M University, College Station, TX, October 26–27, 2004

* Tel.: +1 415 772 5972; fax: +1 415 772 9044.
E-mail address: dmoore@acutech-consulting.com.
URL: www.acutech-consulting.com.

0304-3894/$ – see front matter © 2005 Published by Elsevier B.V.
doi:10.1016/j.jhazmat.2005.07.042

As such, the API/NPRA SVA methodology was seamlessly expanded to include transportation risks simply by applying the methodology to the issue and adapting the technique to the need. The exercise proved that the methodology was scalable to the problem of transportation risks. The end result was simply a presentation of the concept against three transportation risks—a pipeline, a trucking operation, and a rail operation. The second edition, incorporating these changes, was published in 2004. This paper outlines that approach and presents an example.

API and NPRA would like to acknowledge the contribution of the Center for Chemical Process Safety (CCPS) compiled in their "Guidelines for Analyzing and Managing the Security of Fixed Chemical Sites." It was this initial body of work that was used as a basis for developing the first edition of the API NPRA SVA methodology. Although similar in nature, the API/NPRA SVA method was developed for the petroleum and petrochemical industry, at both fixed and mobile systems. Examples have been added that demonstrate applicability at various operating segments of the industry. Owner/operators may want to use any of the methods above, or another equivalent and appropriate methodology in conducting their SVAs. These guidelines should also be considered in light of any applicable federal, state, and local laws and regulations.

2. 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 premise of the guidelines 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 degree of the threat, the degree of vulnerability, the possible consequences of an incident, and the attractiveness of the asset to adversaries.

A basic premise is that all security risks cannot be completely prevented. The security objectives are to employ four basic strategies to help minimize the risk:

1. Deter
2. Detect
3. Delay
4. Respond

Appropriate strategies for managing security can vary widely depending on the individual circumstances of the transportation system, including the type of operation and the threats facing it. As a result, this guideline does not prescribe security measures but instead suggests 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 is not a uniform approach to security in the petroleum industry, and that resources are best applied to mitigate high risk situations primarily.

3. Security vulnerability assessment concepts

3.1. Introduction to SVA terms

A security vulnerability assessment (SVA) is the process that includes determining the likelihood of an adversary successfully exploiting a vulnerability and estimating the resulting degree of damage or impact. Based on this assessment, judgments can be made on degree of risk and the need for additional countermeasures. To conduct a SVA, key terms and concepts must be understood as explained in this chapter.

3.2. Risk definition for SVA

For the purposes of a SVA, the definition of risk is shown in Fig. 1. 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. The complete SVA may evaluate one or more issues or sum the risk of the entire set of security issues. The risk variables are defined as shown in Fig. 2.

For the SVA, the risk of the security event is normally estimated qualitatively. It is based on the consensus judgment of a team of knowledgeable people as to how the likelihood and consequences of an undesired event scenario compares to other scenarios. The assessment is based on best available information, using experience and expertise of the team to

Security Risk is a function of:
- **Consequences** of a successful attack against an asset and
- **Likelihood** of a successful attack against an asset.

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.

Fig. 1. API/NPRA SVA methodology, risk definition.

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 Threat, Vulnerability, and Target Attractiveness.
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, whic h 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.

[1] API

Fig. 2. API/NPRA SVA methodology, SVA risk variables (API).

make sound risk management decisions. The team may use a risk matrix, which is a graphical representation of the risk factors, as a tool for risk assessment decisions.

4. Consequences

The severity of the consequences of a security event at an operation is generally expressed in terms of the degree of injury or damage that would result if there were a successful attack. Malevolent acts may involve effects that are more severe than expected with accidental risk. Some examples of relevant consequences in a SVA include:

- injuries to the public or to workers;
- environmental damage;
- direct and indirect financial losses to the company and to suppliers and associated businesses;
- disruption to the national economy, regional, or local operations and economy;
- loss of reputation or business viability;
- need to evacuate people living or working near the facility;
- excessive media exposure and related public concern affecting people that may be far removed from the actual event location.

The estimate of consequences may be different in magnitude or scope than is normally anticipated for accidental releases. In the case of security events, adversaries are determined to cause maximize damage, so a worse credible security event should be defined. Critical infrastructure especially may have dependencies and interdependencies that need careful consideration.

In addition, theft of hazardous materials should be included in SVAs as applicable. Adversaries may be interested in theft of hazardous materials to either cause direct harm at a later date, use them for other illicit purposes such as illegal drug manufacturing, or possibly to make chemical weapons using the stolen materials as constituents.

Consequences are used as one of the key factors in determining the criticality of the asset and the degree of security countermeasures required. During the facility characterization step, consequences are used to screen low value assets from further consideration. For example, terrorists are assumed to be uninterested in low consequence assets (those that do not meet their criteria for valuable impacts).

5. Asset attractiveness

Not all assets are equally of value to adversaries. A basic assumption of the SVA process is that this perception of value from an adversary's perspective is a factor that influences the likelihood of a security event. Asset attractiveness is an estimate of the real or perceived value of a target to an adversary based on such factors as shown in Fig. 3.

During the SVA, the attractiveness of each asset should be evaluated based on the adversary's intentions or anticipated level of interest in the target. Security strategies can be developed around the estimated targets and potential threats. This factor, along with consequences, are used to screen facilities from more specific scenario analysis and from further specific countermeasures considerations during the first screening of the methodology.

5.1. Threat

Threat can be defined as any indication, circumstance, or event with the potential to cause loss of, or damage, to an asset. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to valued assets. Sources of threats may be categorized as:

- terrorists (international or domestic);
- activists, pressure groups, single-issue zealots;
- disgruntled employees or contractors;
- criminals (e.g., white collar, cyber hacker, organized, opportunists).

Type of effect:
• Potential for causing maximum casualties
• Potential for causing maximum damage and economic loss to the facility and company
• Potential for causing maximum damage and economic loss to the geographic region
• Potential for causing maximum damage and economic loss to the national infrastructure
Type of target:
• Usefulness of the process material as a weapon or to cause collateral damage
• Proximity to national asset or landmark
• Difficulty of attack including ease of access and degree of existing security measures (soft target)
• High company reputation and brand exposure
• Iconic or symbolic target
• Chemical or biological weapons precursor chemical
• Recognizability of the target

Fig. 3. API/NPRA SVA methodology, asset attractiveness factors.

Threat information is important reference data to allow the owner/operator to understand the adversaries interested in the assets of the facility, their operating history, their methods and capabilities, their possible plans, and why they are motivated. This information should then be used to develop a design basis threat or threats.

Adversaries may be categorized as occurring from three general types:

- Insider threats
- External threats
- Insiders working as colluders with external threats

Each applicable adversary type should be evaluated against each asset as appropriate to understand vulnerabilities.

5.2. Vulnerability

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and subsequent destruction or theft of an asset. Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical security, or operational security practices. In a SVA, vulnerabilities are evaluated either by broadly considering the threat and hazards of the assets they could attack or affect, or analyzed by considering multiple potential specific sequences of events (a scenario-based approach). For the API NPRA SVA methodology, each critical asset is analyzed from at least an asset-based approach at first by considering consequences and attractiveness. If it is a specific high value target, then it is recommended to analyze the asset further using scenarios.

5.3. SVA approach

The general approach is to apply risk assessment resources and, ultimately, special security resources primarily where justified based on the SVA results. The SVA process involves consideration of each transportation operation from both the general viewpoint and specific asset viewpoint. Consideration at the general level is useful for determination of overall impacts of loss, infrastructure, and interdependencies at the highest level.

The API/NPRA SVA methodology uses this philosophy in several ways. The method is intended to be comprehensive and systematic in order to be thorough. First, it begins with the SVA team gaining an understanding of the entire operation, the assets that comprise the operation, the critical functions of the operation, and the hazards and impacts if these assets or critical functions are compromised. This results in an understanding of which assets and functions are 'critical' to the business operation.

Criticality is defined both in terms of the potential impact to the workers, community, the environment, and the company, as well as to the business importance of the asset.

Based on this first level of screening from all assets to critical assets, a critical asset/operation list is produced. Next, the critical assets are reviewed in light of the threats. Adversaries may have different objectives, so the critical asset list is reviewed from each adversary's perspective and an asset attractiveness ranking is given. This factor is a quick measure of whether the adversary would value damaging, compromising, or stealing the asset, which serves as an indicator of the likelihood that an adversary would want to attack this asset and why.

If an asset is both critical (based on value and consequences) and attractive, then it is considered a "target" for purposes of the SVA. A target may optionally receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities.

6. API/NPRA security vulnerability assessment methodology

6.1. Overview of the API/NPRA 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

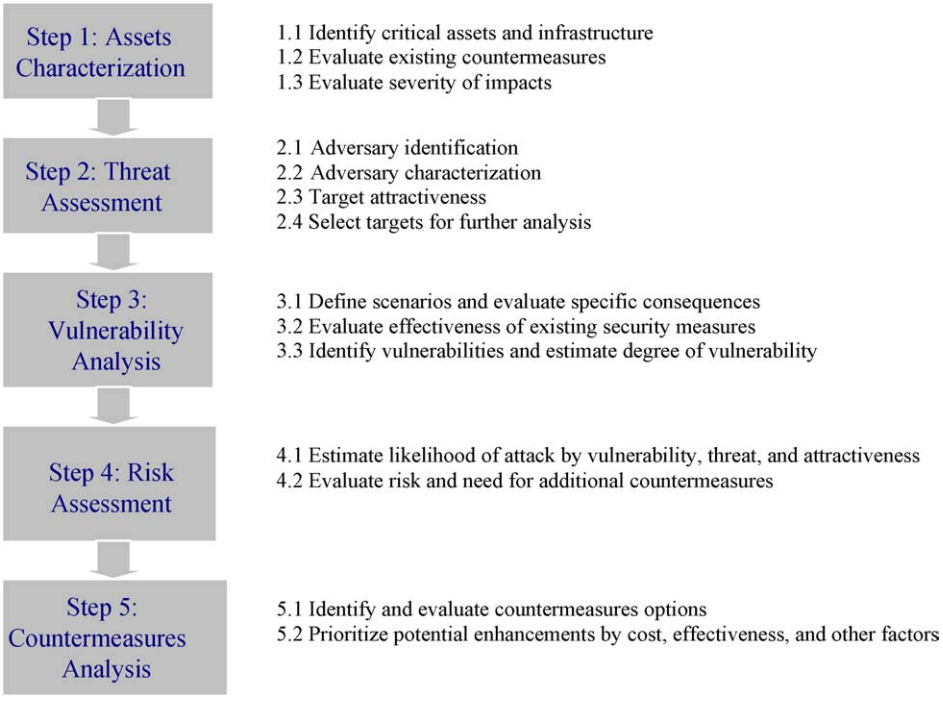

Fig. 4. API/NPRA security vulnerability assessment methodology.

meets the same performance criteria. The overall five-step approach of the API/NPRA SVA methodology is described as follows and is illustrated in Fig. 4:

Step 1. Asset characterization

The asset characterization includes analyzing information that describes the technical details of facility assets as required 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.

Step 2. Threat assessment

The consideration of possible threats should include internal threats, external threats, and internally assisted threats (i.e., collusion between insiders and outside agents). The selection of the threats should include reasonable local, regional, or national intelligence information, where available. This step includes determining the target attractiveness of each asset from each adversary's perspective.

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. It includes the assignment of risk rankings to the security-related scenarios developed. If the asset-based approach is used, the determination of the asset's consequences and attractiveness may be enough to assign a target ranking value and protect via a standard protection set for that target level. In this case, scenarios may not be developed further than the general thought that an adversary is interested in damaging or stealing an asset.

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. Likelihood is determined by the team after considering the attractiveness of the targeted assets assessed under Step 2, the degree of threats assessed under Step 2, and the degree of vulnerability identified under Step 3.

Step 5. Countermeasures analysis

Based on the vulnerabilities identified and the risk that the layers of security are breached, appropriate enhancements to the security countermeasures may be recommended. Countermeasure options will be identified to further reduce

DESCRIPTION	RANKING
A. Possible for any offsite fatalities from large-scale toxic or flammable release; possible for multiple onsite fatalities B. Major environmental impact onsite and/or offsite (e.g., large-scale toxic contamination of public waterway) C. Over $X property damage D. Very long term (> X years) business interruption/expense; Large-scale disruption to the national economy, public or private operations; Loss of critical data; Loss of reputation or business viability	S5 – Very High
A. Possible for onsite fatalities; possible offsite injuries B. Very large environmental impact onsite and/or large offsite impact C. Over $X – $Y property damage D. Long term (X months – Y years) business interruption/expense	S4 – High
A. No fatalities or injuries anticipated offsite; possible widespread onsite serious injuries B. Environmental impact onsite and/or minor offsite impact C. Over $X -$Y property damage D. Medium term (X months – Y months) business interruption/expense	S3 – Medium
A. Onsite injuries that are not widespread but only in the vicinity of the incident location; No fatalities or injuries anticipated offsite B. Minor environmental impacts to immediate incident site area only C. $X – $Y loss property damage D. Short term (up to X months) business interruption/expense	S2 – Low
A. Possible minor injury onsite; No fatalities or injuries anticipated offsite B. No environmental impacts C. Up to $X Property Damage D. Very short term (up to X weeks) business interruption/expense	S1 – Very Low

Fig. 5. API/NPRA SVA methodology, example definitions of consequences of the event.

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 a SVA report that can be used to communicate the results of the SVA to management for appropriate action.

A risk ranking scale can be used to rank the degree of severity. Fig. 5 illustrates a set of consequence definitions based on four categories of events—(A) fatalities and injuries; (B) environmental impacts; (C) property damage; (D) business interruption.

The consequences of a security event at a facility are generally expressed in terms of the degree of acute health effects (e.g., fatality, injury), property damage, environmental effects, etc. This definition of consequences is the same as that used for accidental releases, and is appropriate for security-related events. The key difference is that they may involve effects that are more severe than expected with accidental risk. This difference has been considered in the steps of the SVA. The SVA team should evaluate the potential consequences of an attack using the judgment of the SVA team. If scenarios are done, the specific consequences may be described in scenario worksheets.

Team members skilled and knowledgeable in the process technology should review any off-site consequence analysis data previously developed for safety analysis purposes or prepared for adversarial attack analysis. The consequence analysis data may include a wide range of release scenarios if appropriate.

Proximity to nearby population is a key factor since it is both a major influence on the person(s) selecting a target, and on the person(s) seeking to defend that target. In terms of attractiveness to a terrorist, if the target could expose a large number of persons, this type of target is likely to be a high-value, high-payoff target.

7. Pipeline SVA example

The application of the API/SVA methodology to a typical petroleum liquids pipeline system is illustrated in the following example. Only the first page of each of the four forms is shown for illustrative purposes. It is assumed that the study is conducted by the pipeline company and the various interfaces with customers and suppliers are evaluated but the responsibility for security of those facilities is on the owners (Figs. 6–9).

The general approach is to apply risk assessment resources and, ultimately, special security resources primarily where justified based on the SVA results. The SVA process involves consideration of the pipeline system from both the general

Threat Level	Description
5 – Very High	Indicates that a credible threat exists against the asset and that the adversary demonstrates the capability and intent to launch an attack, and that the subject or similar assets are targeted on a frequently recurring basis.
4 – High	Indicates that a credible threat exists against the asset based on knowledge of the adversary's capability and intent to attack the asset or similar assets.
3 - Medium	Indicates that there is a possible threat to the asset based on the adversary's desire to compromise similar assets.
2 – Low	Indicates that there is a low threat against the asset or similar assets and that few known adversaries would pose a threat to the assets.
1 – Very Low	Indicates no credible evidence of capability or intent and no history of actual or planned threats against the asset or similar assets.

Fig. 6. API/NPRA SVA methodology, threat rating criteria.

Type of effect:
Potential for causing maximum casualties
Potential for causing maximum damage and economic loss to the facility and company
Potential for causing maximum damage and economic loss to the geographic region
Potential for causing maximum damage and economic loss to the national infrastructure
Type of target:
Usefulness of the process material as a weapon or to cause collateral damage
Proximity to national asset or landmark
Difficulty of attack including ease of access and degree of existing security measures (soft target)
High company reputation and brand exposure
Iconic or symbolic target
Chemical or biological weapons precursor chemical
Recognizability of the target

Fig. 7. API/NPRA SVA methodology, target attractiveness factors (for terrorism).

Ranking Levels	Adversary Ranking (1-5)
1 – Very Low	Adversary would have no level of interest in the asset
2 – Low	Adversary would have some degree of interest in the asset
3 – Medium	Adversary would have a moderate degree of interest in attacking the asset
4 – High	Adversary would have a high degree of interest in the asset
5 – Very High	Adversary would have a very high degree of interest in the asset

Fig. 8. API/NPRA SVA methodology, attractiveness factors ranking definitions (A).

viewpoint and specific asset viewpoint. Consideration at the general level is useful for determination of overall impacts of loss, infrastructure, and interdependencies at the system level. The benefit of evaluating specific assets is that individual risks can be evaluated and specific countermeasures applied where justified in addition to more general countermeasures.

For example, all facilities will maintain a minimum level of security with general countermeasures such as the pipeline shutdown and control strategies and administrative security controls. Certain assets will justify a more specific level of security based on their value and expected level of interest to adversaries.

The API/NPRA SVA methodology uses this philosophy in several ways. The method is intended to be comprehensive and systematic in order to be thorough. First, it begins with the SVA team gaining an understanding of the entire pipeline system, the assets that comprise the pipeline system, the critical functions of the pipeline, and the hazards and impacts if these assets or critical functions are compromised. This results in an understanding of which assets and functions are "critical" to the business operation. Criticality may be defined both in terms of the potential impact to the workers, community, the environment and the company, as well as to the business importance and continuity of the system. For example, a pumping station or a specific branch along the pipeline system may be a critical part of the operation of the pipeline system due to inability to operate without it or, if attacked, it has the greatest impact. As such, it may be

Vulnerability Level	Description
5 – Very High	Indicates that there are no effective protective measures currently in place to Deter, Detect, Delay, and Respond to the threat and so an adversary would easily be capable of exploiting the critical asset.
4 – High	Indicates there are some protective measures to Deter, Detect, Delay, or Respond to the asset but not a complete or effective application of these security strategies and so it would be relatively easy for the adversary to successfully attack the asset.
3 – Medium	Indicates that although there are some effective protective measures in place to Deter, Detect, Delay, and Respond, there isn?t a complete and effective application of these security strategies and so the asset or the existing countermeasures could likely be compromised.
2 – Low	Indicates that there are effective protective measures in place to Deter, Detect, Delay, and Respond, however, at least one weakness exists that an adversary would be capable of exploiting with some effort to evade or defeat the countermeasure given substantial resources.
1 – Very Low	Indicates that multiple layers of effective protective measures to Deter, Detect, Delay, and Respond to the threat exist and the chance that the adversary would be able to exploit the asset is very low.

(A)

		SEVERITY				
		5	4	3	2	1
LIKELIHOOD	5	High	High	High	Med	Med
	4	High	High	Med	Med	Low
	3	High	Med	Med	Low	Low
	2	Med	Med	Low	Low	Low
	1	Med	Low	Low	Low	Low

(B)

Fig. 9. (A) API/NPRA SVA methodology, vulnerability rating criteria. (B) API/NPRA SVA methodology, risk ranking matrix.

given a high priority for further analysis and special security countermeasures.

Based on this first level of screening from all assets to critical assets, a critical asset list is produced. Next, the critical assets are reviewed in light of the threats. Adversaries may have different objectives, so the critical asset list is reviewed from each adversary's perspective and an asset attractiveness ranking is given. This factor is a quick measure of whether the adversary would value damaging, compromising, or stealing the asset, which serves as an indicator of the likelihood that an adversary would want to attack this asset and why.

If an asset is both critical (based on value and consequences) and attractive, then it is considered a "target" for purposes of the SVA. A target may optionally receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities. As shown in Fig. 10, all assets receive at least a general security review. This is accomplished by the basic SVA team's consideration as an asset to begin with, along with a baseline security survey. General security considerations may be found in security references such as the countermeasures checklist provided in the API/NPRA SVA guidelines.

The study is conducted in a top-down, systematic manner following the logic flowchart for the SVA as shown in Fig. 11. The five steps of the process are documented in four forms:

Form 1—critical assets/criticality form

Determine the major assets of the pipeline system including control rooms, gates and access control points, marine terminals, communications networks, terminus points for export and import pipelines, utilities, and supporting infrastructure. All entry points to critical facilities should be evaluated as an asset in order to focus the analysis on the need for perimeter security and access control. The team lists all relevant assets on Form 1 in column 1. Similar assets within a facility with similar geographic locations on the property, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set. In column 2, document the design basis of the asset and the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen. In column, 3 rank the estimated overall severity of the loss of the asset. Use the five-level severity ranking scale for severity or develop an equivalent as required for the particular facility. Following the determination of

Facility name: 1. ACME Pipeline Company

Critical assets form

Critical assets	Criticality/hazards	Asset severity ranking
1. Main line, 24-in. liquids pipeline system—1000 miles, provides 500,000 b/d. Finished products; gasoline, jet fuel and home heating oil. Thirty-five main-line block valves (approximately every 50 miles), 20 booster (pumping) stations, traverses primarily rural areas	Main line serves large metropolitan areas. Several million retail customers plus five major international airports and two large military installations. Includes a major above ground river crossing, which provides drinking water to large urban community	5
2. ABC branch—10 miles, 8 in. branch line serving mixed products to marketing terminal serving a rural population	Serves rural customer base. No national defense impact. Remotely located and no major environmental impacts. Alternative delivery sources available.	1
3. DEF branch and inter-modal terminal—branch line providing mixed products to multi-modal marketing terminal, breakout facility, interconnection to other pipelines, and direct connect to military, commercial airports, and power plant	Possible onsite fatalities. Possible offsite environmental impact. Limited alternative delivery resources to customers.	4
4. Endpoint storage facility—major tank farm for large metropolitan area, airport, and other party pipeline connection.	Serves large metropolitan area. Several million retail customers plus major international airport. Area served by other sources. Located in a sparsely populated industrial area.	2
5. River span block valve	Block valve is upstream from above ground river span (see item 7). Breach could cause release of pipe volume into river and impact public safety and significant contamination to the water supply of a major metropolitan center. Restoration costs significant due to river spill clean up and difficult access to valve. Short timeframe to repair.	5
6. River span pipeline (above ground)	Above ground river span (see 1 above). Breach could release significant product into river and contaminate public water supply to a major metropolitan center. Block valve used as active mitigation, if not damaged. Significant public safety concern due to frequent recreational and commercial use on river. Long-term repair timeframe and significant repair costs and spill clean up costs. No alternate mode to market. Significant service interruption.	5
7. Inter-modal terminal	Large inter-modal products terminal with rail, truck, and pipeline service. Serves large metropolitan area. Provides gasoline to retail market, jet fuel to two major international airports and USAF. Large-scale damage would take months to repair. Repair costs would be significant. Significant disruption to local economy and possible national defense. No significant environmental impact. Limited public safety and employee impact.	4

Form 2—threats worksheet

Document the threats against the pipeline system or a critical facility on Form 2. Include consideration in column 1 of general types of adversaries that will be considered (usually terrorists, disgruntled employee or contractor, or extreme activist as an example, but more specific or other groups can be considered as required); column 2 is the source of the attack (EXT, external to the pipeline/facility; INT, internal to the pipeline/facility); column 3 documents the threat specific to the pipeline/facility being evaluated; column 4 documents the specific or general threat of that type of adversary against this or similar assets worldwide; column 5 documents the potential actions that the adversary could take; column 6 documents the assumed capabilities, weapons, tactics, and sophistication of the adversary; column 7 documents their level of motivation; column 8 provides for an overall ranking assessment per the threat ranking scale or equivalent.

Facility name: 1. ACME Pipeline Company

Adversary types	Source	Site specific threat	Threat history	Potential actions	Adversary capability	Adversary motivation	Threat ranking
International terrorists	**I/E/C**	No site-specific history of international terrorism	There have been numerous international terrorist acts against petroleum pipelines in the world to date. Most notably in South America and Middle East. U.S. Homeland Security Advisory System is rated orange presently. According to recent FBI reports, Al Qaeda continues to show interest in the energy sector and large scale operations that have significant impacts to public safety, the national economy, and national symbol of American might and wealth	Use of stealth or force to cause damage and/or release of hydrocarbons. Possible theft or contamination of product possible but not likely. Degradation of assets and interruption of service biggest concern. Possible environmental release into public water supply and public safety are concerns. Damage to equipment and time to repair are also issues	High level of organizational support; good resources; good financial backing; network of members; highly developed communication capabilities; weapons including small arms and explosives; possible vehicle bomb based on past events	Assume adversary is highly motivated, likely extremist, prepared to die for their cause with intent to cause maximum damage to company assets including loss of life and economic disruption	4

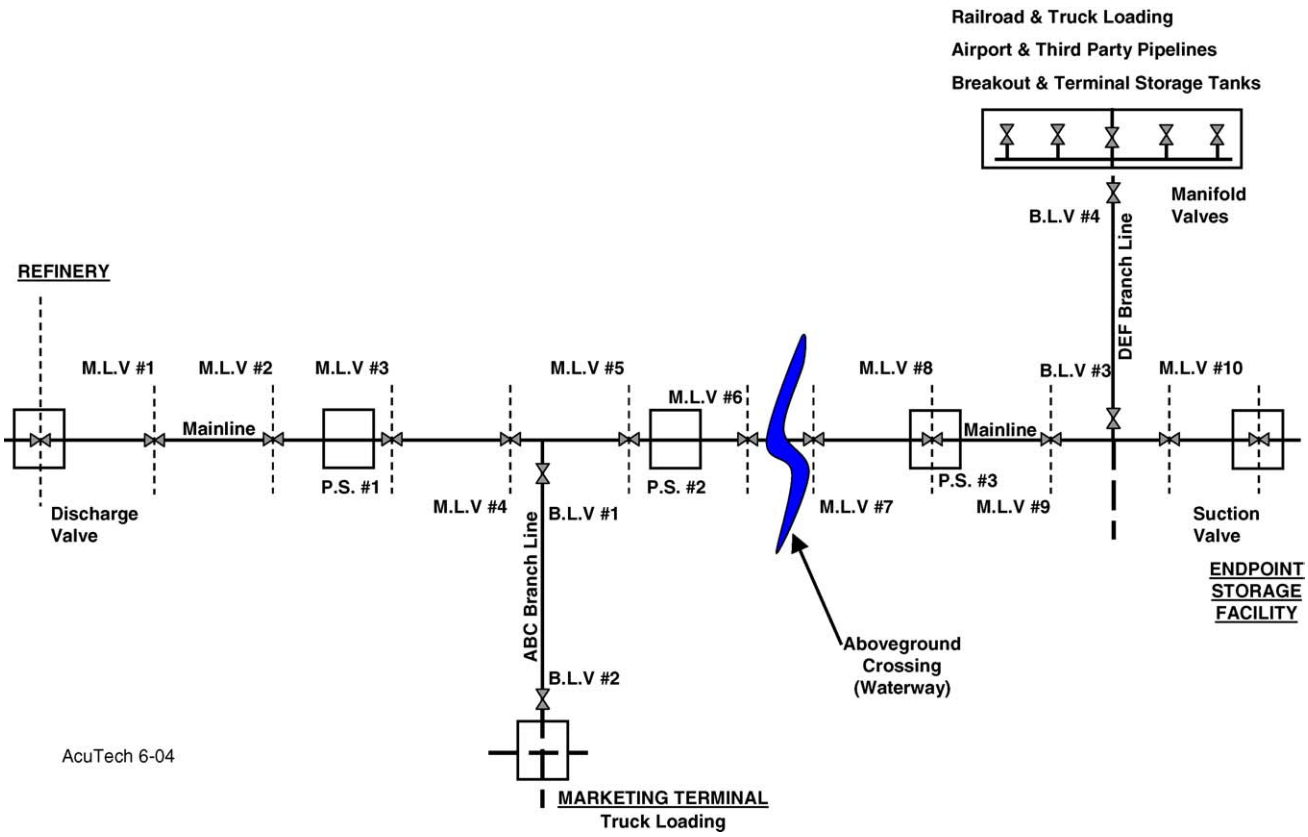

Fig. 10. API/NPRA SVA pipeline example.

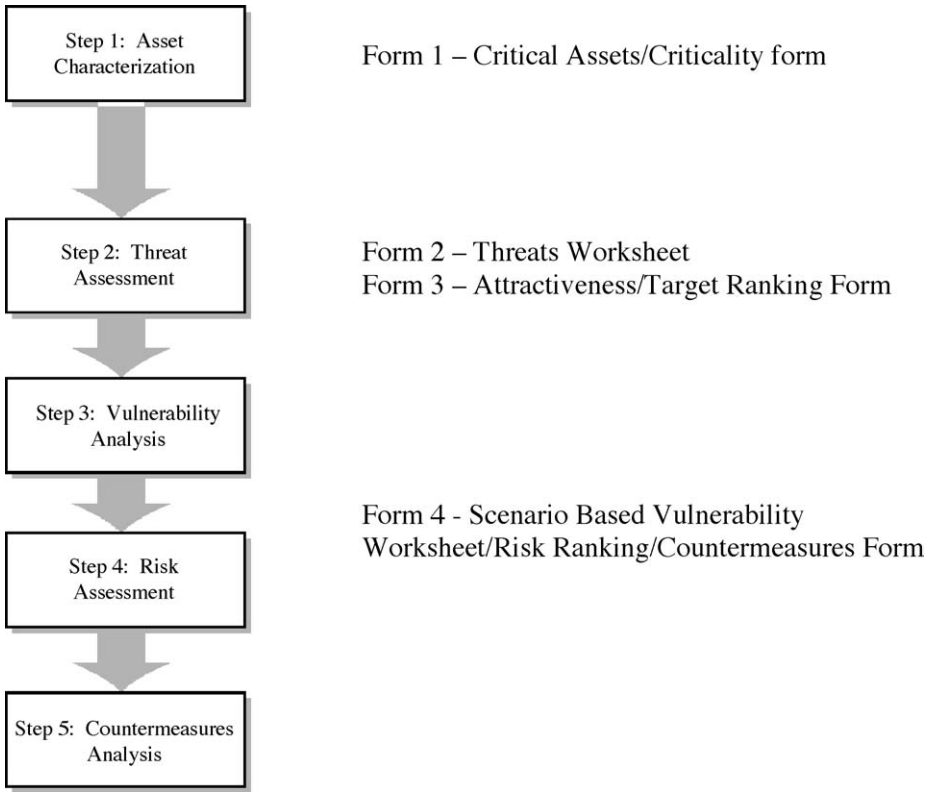

Fig. 11. API/NPRA SVA methodology flow diagram.

Adversary types	Source	Site specific threat	Threat history	Potential actions	Adversary capability	Adversary motivation	Threat ranking
Domestic terrorist or activist	**I/E/C**	History at the main-line system of multiple bomb threats over the past 2 years. All concluded were fakes	No confirmed domestic acts of terrorism on the pipeline infrastructure	Possible for a disruptive event from domestic terrorist such as bombing or disruption of operations	Low level of organizational support; poor resources and financial backing; small network of members; cell phone/email communication capabilities; weapons including small arms and explosives	Adversary intent is to cause economic harm through service interruption. If domestic terrorist, intent and motivation could be extreme to cause maximum damage, possibly without personal sacrifice	3
Disgruntled employee or contractor	**INT**	No evidence of sabotage has been discovered in the past	Minimal acts of sabotage or workplace violence	Sabotage to equipment including SCADA causing possible release of hazardous materials, contamination of products, environmental impact, or major equipment damage and business interruption. Possible for nuisance threats, particularly from contract workers with intent to disrupt operations	Insider access, knowledge, and ability to operate independently with authorization and without question. May have access to keys, computer passwords, gate access codes, communication equipment, records, vehicles, proximity cards for access cards, company process control system	Nuisance adversary is intent to cause inconvenience and financial impacts to the company or their employer. If very disgruntled or troubled, intent and motivation could be extreme to cause maximum damage, possibly with personal sacrifice as evidenced in various national workplace violence cases	4

Form 3—attractiveness/target ranking form

Columns 1–3 are repeated from Form 1 for reference. Column 4 is a documented rationale for why the particular asset is attractive (or unattractive) and column 5 is a ranking of that attractiveness on a relative attractiveness ranking scale or equivalent. This is repeated for other adversaries. Column 10 is an overall target ranking per the same scale, and is normally considered to be the highest attractiveness of any of the individual adversary rankings but also considers that the sum the different adversary's interests may make the asset more attractive. The target ranking is used to judge the degree of attractiveness of the target considering all the adversaries.

Facility name: 1. ACME Pipeline Company

Critical assets	Function/hazards/ criticality	S	Asset attractiveness						
			Foreign/domestic attractiveness rationale	A1	Employee/ contractor attractiveness rationale	A2	Activist attractiveness rationale	A3	TR
1. Main line, 24-in. liquids pipeline system—1000 miles, provides 500,000 b/d. Finished products; gasoline, jet fuel, and home heating oil. Thirty-five main-line block valves (approximately every 50 miles), 20 booster (pumping) stations, traverses primarily rural areas	Serves rural customer base. No national defense impact. Remotely located and no major environmental impacts. Alternative delivery sources available	5	Easy access due to length of pipeline and location in a rural area with several above ground-unmanned pumping stations. Minimal disruptions to only a rural customer base no impact to military and minimal potential environmental impact	1	Some insider insight helpful but not necessary	2	Limited interest	2	TR2

Critical assets	Function/hazards/ criticality	S	Asset attractiveness						
			Foreign/domestic attractiveness rationale	A1	Employee/ contractor attractiveness rationale	A2	Activist attractiveness rationale	A3	TR
2. ABC branch—10 miles, 8 in. branch line serving mixed products to marketing terminal serving a rural population	Main line serves large metropolitan areas. Several million retail customers plus five major international airports, and two large military installations. Includes a major above ground river crossing, which provides drinking water to large urban community	1	Major disruption to residential, air travel, and military. Public safety and drinking water contamination. Easy access	2	Some insider insight helpful but not necessary	2	Public image impact due to press/media interest	3	TR3
3. DEF branch and inter-modal terminal—branch line providing mixed products to multi-modal marketing terminal, breakout facility, interconnection to other pipelines, and direct connect to military, commercial airports, and power plant	Possible onsite fatalities. Possible offsite environmental impact. Limited alternative delivery resources to customers	4	Major disruption to air travel, power supply, and military. Easy access	3	Some insider insight helpful but not necessary	2	Public image impact due to press/media interest	3	TR3
4. Endpoint storage facility —major tank farm for large metropolitan area, airport and other party pipeline connection	Serves large metropolitan area. Several million retail customers plus major international airport. Area served by other sources. Located in a sparsely populated industrial area.	2	Hardened facility. Access difficult but impact significant	3	Insider information very helpful both to gain access and operational	2	Nuisance issue with trespassing. Public image impact. Operational knowledge needed	2	TR3
5. River span block valve	Block valve is upstream from above ground river span (see item 7). Breach could cause release of pipe volume into river and impact public safety and significant contamination to the water supply of a major metropolitan center. Restoration costs significant due to river spill clean up and difficult access to valve. Short timeframe to repair	5	Public safety and drinking water contamination. Perhaps included with attack on asset-river span (above ground)	2	Some insider insight helpful but not necessary. Difficult access within minimal success	1	Limited interest	2	TR2
6. River span pipeline (above ground)	Above ground river span (see 1 above). Breach could release significant product into river and contaminate public water supply to a major metropolitan center. Block valve used as active mitigation, if not damaged. Significant public safety concern due to frequent recreational and commercial use on river. Long-term repair timeframe and significant repair costs and spill clean up costs. No alternate mode to market. Significant service interruption	5	Public safety and drinking water contamination. Easy access	3	No insider knowledge needed for breach/access	1	Public image impact due to press/media interest	3	TR3

Critical assets	Function/hazards/ criticality	S	Asset attractiveness						
			Foreign/domestic attractiveness rationale	A1	Employee/ contractor attractiveness rationale	A2	Activist attractiveness rationale	A3	TR
7. Inter-modal terminal	Large inter-modal products terminal with rail, truck, and pipeline service. Serves large metropolitan area. Provides gasoline to retail market, jet fuel to two major international airports and USAF. Large-scale damage would take months to repair. Repair costs would be significant. Significant disruption to local economy and possible national defense. No significant environmental impact. Limited public safety and employee impact	4	Hardened facility. Access difficult but impact significant	3	Insider information very helpful both to gain access and operational	2	Nuisance issue with trespassing. Public image impact. Operational knowledge needed	2	TR3

Form 4—scenario based vulnerability worksheet/risk ranking/countermeasures form

Column 1 is the security event type (generally one of four security events including loss of containment, degradation of the asset, theft, or contamination); column 2 is the threat category (adversary type such as terrorist, activist, employee); column 3 is the type of adversary attack (insider/external); column 4 is the undesired act (the assumed attack scenario, generally taken from the threats worksheet columns 5, 6, 7); column 5 is the consequences; column 6 (s) is the severity ranking from the severity ranking scale; column 7 is the existing countermeasures, which considers the deter, detect, delay, and respond philosophy; column 8 is the vulnerability, which also considers the weaknesses or missing elements of the security strategy specific to the scenario; column 9 is the vulnerability ranking per the vulnerability ranking scale; column 10 is the likelihood ranking (L) using the likelihood scale, which is a judgment of the team considering the factors of vulnerability, threat, and attractiveness; column 11 is the risk ranking (R) per the referenced risk ranking matrix values; column 12 is the new/countermeasures suggestions (where the risk is considered significant enough to justify the need for change).

Facility name: 1. ACME Pipeline Company
Critical assets: 6. River span pipeline (above ground)

Scenario worksheet form

Security event type	Threat category	Type	Undesired act	Consequences	S	Existing safeguards/ countermeasures	Vulnerability	V	L	R	Recommendations
1.1. Destruction of span, release of product and loss of containment	Terrorist	I/E/C	Destruction of river span by bombing	Damage of river span; release of product into river; contamination of public drinking water supply; loss of service to downstream facilities for an extended period	S5	1.1. Fencing around cable platform	1. There are some protective measures; river span remote; easy access - above grade	4	L3	High	1. Consider additional fencing to prevent access to river span
						1.2. Air patrol and ground observation					2. Consider intrusion/motion detection along this exposed section of pipeline
						1.3. Manually operated block valve					3. Consider CCTV at the river crossing
						1.4. Monitoring pipeline conditions and flow ctrl					4. Consider increasing land and air patrol at higher threat levels including both employee and local law enforcement.
Critical Assets: 7. Inter-modal terminal											
1.1. Destruction of inter-modal terminal manifold piping	Terrorist	I/E/C	Destruction of piping by bombing	Inability to receive or pump product and possible onsite fatalities	S4	1.1. Fencing, lighting, access control, CCTV, manned 24/7, security procedures in place	1. There are multiple protective measures but at least one weakness to gain access	2	L3	Med	5. Consider improved access control, 24/7 security guards at higher threat levels 6. Consider one or more of the following: secondary fencing; intrusion detection alarms background checks; vehicle inspection

8. Responsibilities

This example includes a sampling of assets that may be owned or operated by various parties. The responsibilities for conducting the SVA and for providing security need to be determined and may not solely be with the pipeline owner/operator. It is recommended that the SVA include the appropriate parties to fully analyze the security issues, and that the results are discussed with owner/operators of adjacent facilities and infrastructure providers as required for risk communication and completeness.

9. Conclusions

The analysis of a company's security risks is not complete unless the entire value chain is evaluated. This may include truck, rail, or pipeline transportation of hazardous materials.

A common methodology was proven to be useful for the evaluation of both facility and transportation risks. As such, the API/NPRA SVA methodology was seamlessly expanded to include transportation risks simply by applying the methodology to the issue and adapting the technique to the need. The exercise proved that the methodology was scalable to the problem of transportation risks. The end result was simply a presentation of the concept against three transportation risks—a pipeline, a trucking operation, and a rail operation.