

October 2004

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition



October 2004

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

American Petroleum Institute
1220 L Street, NW
Washington, DC
20005-4070

National Petrochemical &
Refiners Association
1899 L Street, NW
Suite 1000
Washington, DC
20036-3896

All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 1220 L Street, N.W., Washington, D.C. 20005.

Copyright © 2004 American Petroleum Institute

PREFACE

The American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) are pleased to make this Second Edition of this Security Vulnerability Assessment Methodology available to members of petroleum and petrochemical industries. The information contained herein has been developed in cooperation with government and industry, and is intended to provide a tool to help maintain and strengthen the security of personnel, facilities, and industry operations; thereby enhancing the security of our nation's energy infrastructure.

API and NPRA wish to express sincere appreciation to the member companies who have made personnel available to work on this document. We especially thank the Department of Homeland Security and its Directorate of Information Analysis & Infrastructure Protection and the Department of Energy's Argonne National Laboratory for their invaluable contributions. The lead consultant in developing this methodology has been David Moore of the AcuTech Consulting Group, whose help and experience was instrumental in developing this document. Lastly, we want to acknowledge the contributions of the Centers for Chemical Process Safety for their initial work on assessing security vulnerability in the chemical industry.

This methodology constitutes but one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities. However, there are several other vulnerability assessment techniques and methods available to industry, all of which share common risk assessment elements. Many companies, moreover, have already assessed their own security needs and have implemented security measures they deem appropriate. This document is not intended to supplant measures previously implemented or to offer commentary regarding the effectiveness of any individual company efforts.

The focus of this second edition was to expand the successful first edition by including additional examples of how the methodology can be applied to a wide range of assets and operations. This includes petroleum refining and petrochemical manufacturing operations, pipelines, and transportation including truck and rail. The methodology was originally field tested at two refinery complexes, including an interconnected tank farm, marine terminal and lube plant before the publication of the first edition. Since then, it has been used extensively at a wide variety of facilities involving all aspects of the petroleum and petrochemical industries.

API and NPRA are not undertaking to meet the duties of employers, manufacturers, or suppliers to train and equip their employees, nor to warn any who might potentially be exposed, concerning security risks and precautions. Ultimately, it is the responsibility of the owner or operator to select and implement the security vulnerability assessment method and depth of analysis that best meet the needs of a specific location.

CONTENTS

CHAPTER 1 INTRODUCTION	1
1.1 INTRODUCTION TO SECURITY VULNERABILITY ASSESSMENT.....	1
1.2 OBJECTIVES, INTENDED AUDIENCE AND SCOPE OF THE GUIDANCE	1
1.3 SECURITY VULNERABILITY ASSESSMENT AND SECURITY MANAGEMENT PRINCIPLES.....	2
CHAPTER 2 SECURITY VULNERABILITY ASSESSMENT CONCEPTS	3
2.1 INTRODUCTION TO SVA TERMS	3
2.2 RISK DEFINITION FOR SVA.....	3
2.3 CONSEQUENCES.....	4
2.4 ASSET ATTRACTIVENESS.....	4
2.5 THREAT.....	5
2.6 VULNERABILITY	5
2.7 SVA APPROACH.....	5
2.8 CHARACTERISTICS OF A SOUND SVA APPROACH.....	7
2.9 SVA STRENGTHS AND LIMITATIONS	8
2.10 RECOMMENDED TIMES FOR CONDUCTING AND REVIEWING THE SVA.....	8
2.11 VALIDATION AND PRIORITIZATION OF RISKS.....	8
2.12 RISK SCREENING.....	9
CHAPTER 3 SECURITY VULNERABILITY ASSESSMENT METHODOLOGY	9
3.1 OVERVIEW OF THE SVA METHODOLOGY	9
3.2 SVA METHODOLOGY	15
3.3 STEP 1: ASSETS CHARACTERIZATION.....	18
3.4 STEP 2: THREAT ASSESSMENT.....	23
3.5 SVA STEP 3: VULNERABILITY ANALYSIS	25
3.6 STEP 4: RISK ANALYSIS/RANKING.....	28
3.7 STEP 5: IDENTIFY COUNTERMEASURES:.....	28
3.8 FOLLOW-UP TO THE SVA.....	29
ATTACHMENT 1 – EXAMPLE SVA METHODOLOGY FORMS	31
ABBREVIATIONS AND ACRONYMS	41
APPENDIX A—SVA SUPPORTING DATA REQUIREMENTS.....	43
APPENDIX B—SVA COUNTERMEASURES CHECKLIST	45
APPENDIX C—SVA INTERDEPENDENCIES AND INFRASTRUCTURE CHECKLIST.....	67
APPENDIX C1—REFINERY SVA EXAMPLE	115
APPENDIX C2—PIPELINE SVA EXAMPLE	123
APPENDIX C3—TRUCK TRANSPORTATION SVA EXAMPLE	135
APPENDIX C4—RAIL TRANSPORTATION SVA EXAMPLE	145
References	155
Figures	
2.1 Risk Definition	3
2.2 SVA Risk Variables	3
2.3 Asset Attractiveness Factors	4
2.4 Overall Asset Screening Approach.....	6
2.5 Recommended Times for Conducting and Reviewing the SVA	9

3.1	Security Vulnerability Assessment Methodology Steps	11
3.1a	Security Vulnerability Assessment Methodology—Step 1	12
3.1b	Security Vulnerability Assessment Methodology—Step 2.....	13
3.1c	Security Vulnerability Assessment Methodology—Steps 3 – 5	14
3.2	SVA Methodology Timeline	15
3.3	SVA Team Members	16
3.4	Sample Objectives Statement	16
3.5	Security Events of Concern	17
3.6	Description of Step 1 and Substeps	19
3.7	Example Candidate Critical Assets	20
3.8	Possible Consequences of Security Events	21
3.9	Example Definitions of Consequences of the Event.....	22
3.10	Description of Step 2 and Substeps	23
3.11	Threat Rating Criteria.....	25
3.12	Target Attractiveness Factors (for Terrorism)	25
3.13	Attractiveness Factors Ranking Definitions (A).....	26
3.14	Description of Step 3 and Substeps	26
3.15	Vulnerability Rating Criteria	27
3.16	Description of Step 4 and Substeps	28
3.17	Risk Ranking Matrix	29
3.18	Description of Step 5 and Substeps	29
A	SVA Methodology Flow Diagram	124

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries

Chapter 1 Introduction

1.1 INTRODUCTION TO SECURITY VULNERABILITY ASSESSMENT

The first step in the process of managing security risks is to identify and analyze the threats and the vulnerabilities facing a facility by conducting a Security Vulnerability Assessment (SVA). The SVA is a systematic process that evaluates the likelihood that a threat against a facility will be successful. It considers the potential severity of consequences to the facility itself, to the surrounding community and on the energy supply chain.

The SVA process is a team-based approach that combines the multiple skills and knowledge of the various participants to provide a complete security analysis of the facility and its operations. Depending on the type and size of the facility, the SVA team may include individuals with knowledge of physical and cyber security, process safety, facility and process design and operations, emergency response, management and other disciplines as necessary.

The objective of conducting a SVA is to identify security hazards, threats, and vulnerabilities facing a facility, and to evaluate the countermeasures to provide for the protection of the public, workers, national interests, the environment, and the company. With this information security risks can be assessed and strategies can be formed to reduce vulnerabilities as required. SVA is a tool to assist management in making decisions on the need for countermeasures to address the threats and vulnerabilities.

1.2 OBJECTIVES, INTENDED AUDIENCE AND SCOPE OF THE GUIDANCE

This document was prepared by the American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) Security Committees to assist the petroleum and petrochemical industries in understanding security vulnerability assessment and in conducting SVAs. The guidelines describe an approach for assessing security vulnerabilities that is widely applicable to the types of facilities operated by the industry and the security issues they face. During the development process it was field tested at two refineries, two tank farms, and a lube plant, which included typical process equipment, storage tanks, marine operations, infrastructure, pipelines, and distribution terminals for truck and rail. Since then, it has been used extensively at a wide variety of facilities involving all aspects of the petroleum and petrochemical industry.

This methodology constitutes one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities. However, there are several other vulnerability assessment techniques and methods available to industry, all of which share common risk assessment elements. Many companies, moreover, have already assessed their own security needs and have implemented security measures they deem appropriate. This document is not intended to supplant measures previously implemented or to offer commentary regarding the effectiveness of any individual company efforts.

Ultimately, it is the responsibility of the owner/operator to choose the SVA method and depth of analysis that best meets the needs of the 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 activities:

- Characterize the facility to understand what critical assets need to be secured, their importance and their interdependencies and supporting infrastructure;
- Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each adversary and the consequences if they are damaged or stolen;
- Identify potential security vulnerabilities that threaten the asset'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 to ensure adequate countermeasures are being applied.

This guidance was developed for the industry as an adjunct to other available references which includes:

- American Petroleum Institute, "Security Guidelines for the Petroleum Industry", May, 2003;
- API RP 70, "Security for Offshore Oil and Natural Gas Operations", First Edition, April, 2003;

- “Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites”, American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), August, 2002;
- “Vulnerability Analysis Methodology for Chemical Facilities (VAM-CF)”, Sandia National Laboratories, 2002.

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 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.

The guidance is intended for site managers, security managers, process safety managers, and others responsible for conducting security vulnerability analyses and managing security at petroleum and petrochemical facilities.

The method described in this guidance may be widely applicable to a full spectrum of security issues, but the key hazards of concern are malevolent acts, such as terrorism, that have the potential for widespread casualties or damage.

These guidelines provide additional industry segment specific guidance to the overall security plan and SVA method presented in Part I of the API Security Guidelines for the Petroleum Industry.

1.3 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 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. 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 necessarily a quantitative risk assessment, but are usually 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.

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 facility, including the type of facility and the threats facing the facility. 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 isn't a uniform approach to security in the petroleum industry, and that resources are best applied to mitigate high-risk situations primarily.

All Owner/Operators are encouraged to seek out assistance and coordinate efforts with federal, state, and local law enforcement agencies, and with the local emergency services and Local Emergency Planning Committee. Owner/Operators can also obtain and share intelligence, coordinate training, and tap other resources to help deter attacks and to manage emergencies.

Chapter 2 Security Vulnerability Assessment Concepts

2.1 INTRODUCTION TO SVA TERMS

A Security Vulnerability Assessment (SVA) is the process that includes determining the likelihood of an adversary successfully exploiting 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.

2.2 RISK DEFINITION FOR SVA

For the purposes of a SVA, the definition of risk is shown in Figure 2.1. 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 Figure 2.2.

A high-risk event, for example, is one which is represented by a high likelihood of a successful attack against a given critical target asset. Likelihood is determined by considering several factors including its attractiveness to the adversary, the degree of threat, and the degree of vulnerability. Criticality is determined by the asset's importance or value, and the potential consequences if attacked. If the likelihood of a successful attack against an important asset is high, then the risk is considered high and appropriate countermeasures would be required for a critical asset at high risk.

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 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.

The API NPRA SVA Methodology has a two step screening process to focus attention on higher risk events. The key variables considered in the first screening are Consequences and Target Attractiveness. If either of those are either not sufficiently significant, the asset is screened out from further specific consideration. Later, the complete set of risk variables shown in Figure 2.1 are used in the second screen to determine the need for additional specific countermeasures.

Figure 2.1—Risk Definition

Security Risk is a function of: <ul style="list-style-type: none"> • Consequences of a successful attack against an asset and • Likelihood of a successful attack against an asset.
Likelihood is a function of: <ul style="list-style-type: none"> • the Attractiveness to the adversary of the asset, • the degree of Threat posed by the adversary, and • the degree of Vulnerability of the asset.

Figure 2.2—SVA Risk Variables⁴

Consequences	<i>Consequences</i> are the potential adverse impacts to a facility, the local community and/or the nation as a result of a successful attack.
Likelihood	<i>Likelihood</i> 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 (see Figure 2.1).
Attractiveness	<i>Attractiveness</i> is a surrogate measure for likelihood of attack. This factor is a composite estimate of the perceived value of a target to a specific adversary.
Threat	<i>Threat</i> is a function of an adversary's intent, motivation, capabilities, and known patterns of operation. Different adversaries may pose different threats to various assets within a given facility or to different facilities.
Vulnerability	<i>Vulnerability</i> is 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.

⁴Ibid, AICHe.

2.3 CONSEQUENCES

The severity of the consequences of a security event at a facility 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).

2.4 ASSET ATTRACTIVENESS

Not all assets are of equal 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 Figure 2.3.

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.

Figure 2.3—Asset Attractiveness Factors

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 a 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
• Recognition of the target

2.5 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).

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.

2.6 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 this 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.

2.7 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 facility 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 facility level, and outer perimeter analysis including access control and general physical security. For example, all facilities will maintain a minimum level of security with general countermeasures such as the plant access control strategy and administrative controls. Certain assets will justify a more specific level of security, such as additional surveillance or barriers, based on their value and expected level of interest to adversaries. 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.

This 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 facility, the assets that comprise the facility, the critical functions of the facility, 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. This is illustrated in Figure 2.4.

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. For example, a storage tank of a hazardous material may not be the most critical part of the operation of a process, but if attacked, it has the greatest combined impact so it may be 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 Figure 2.4, all assets receive at least a general security review. This is accomplished by the SVA team’s initial consideration of assets, along with a baseline security survey. General security considerations may be found in security references such as the countermeasures checklist provided in Appendix B.

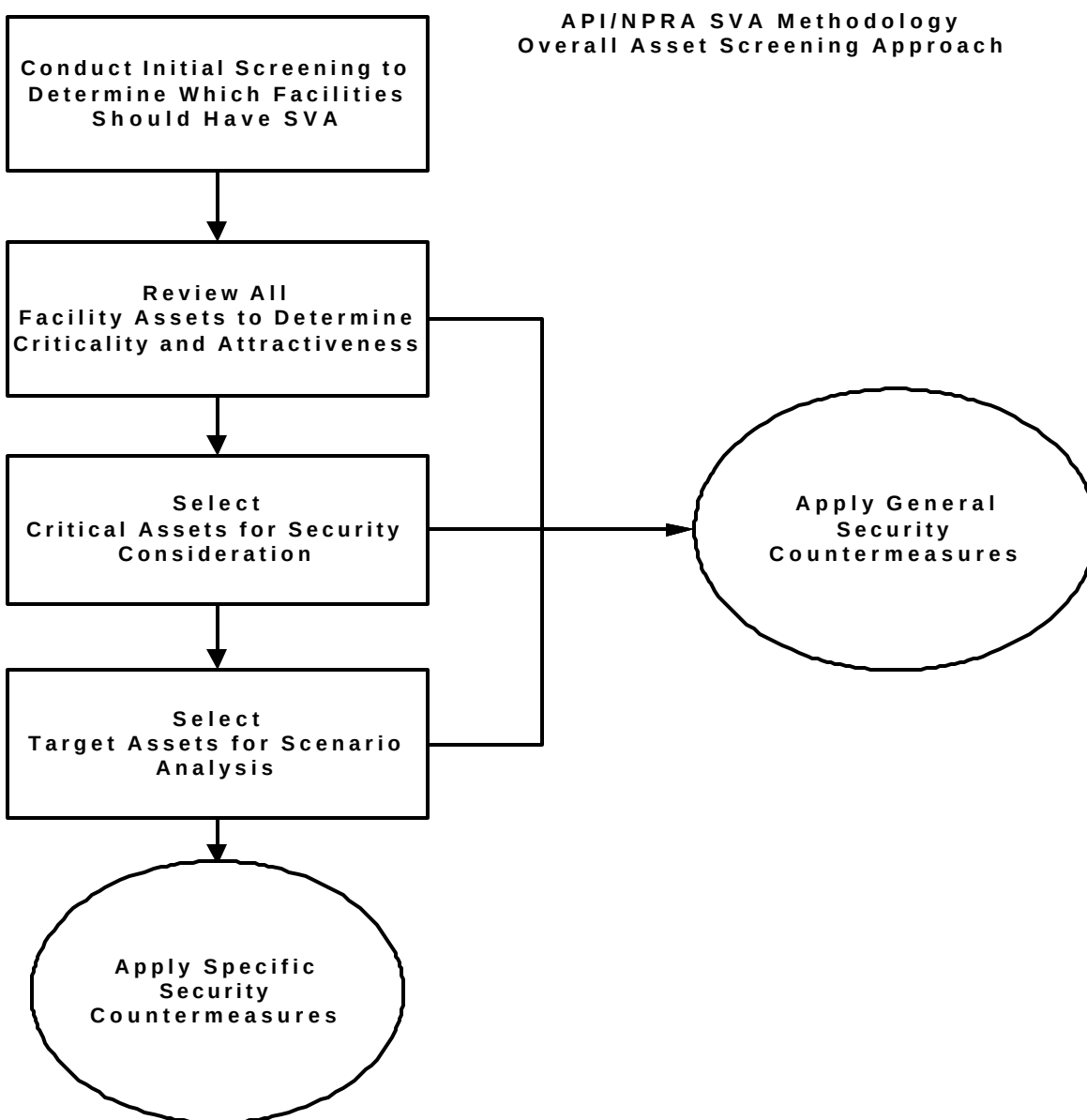


Figure 2.4—Overall Asset Screening Approach

All facilities should establish a security strategy. The general strategy is to protect against unauthorized access at the facility perimeter, and to control the access of authorized persons on the facility. Certain assets will be protected with added layers of protection, due to their attractiveness and consequences of loss. The specific security countermeasures provided to those assets would be to deter, detect, delay, and respond to credible threats against the assets to limit the risk to a certain level.

2.8 CHARACTERISTICS OF A SOUND SVA APPROACH

It is important to distinguish between a security risk management process and any given SVA methodology. Security risk management is the management framework that includes the SVA, development and implementation of a security plan, and the application of needed countermeasures to enhance security. SVA is the estimation of risk for the purposes of decision-making. SVA methodologies can be very powerful analytical tools to integrate data and information, and help understand the nature and locations of risks of a system. However, SVA methods alone should not be relied upon to establish risk, nor solely determine decisions about how risks should be addressed. SVA methods should be used as part of a process that involves knowledgeable and experienced personnel that critically review the input, assumptions, and results. The SVA team should integrate the SVA output with other factors, the impact of key assumptions, and the impact of uncertainties created by the absence of data or the variability in assessment inputs before arriving at decisions about risk and actions to reduce risk.

A variety of different approaches to SVA have been employed in the petroleum sector as well as other industries. The major differences among approaches are associated with:

- The relative “mix” of knowledge, data, or logic SVA methods;
- The complexity and detail of the SVA method; and
- The nature of the output (probabilistic versus relative measures of risk).

Ultimately, it is the responsibility of the owner/operator to choose the SVA method that best meets the needs of the company, the facilities and the agencies tasked with providing additional security in times of imminent danger. Therefore, it is in the best interest of the owner/operator to develop a thorough understanding of the various SVA methods in use and available, as well as the respective strengths and limitations of the different types of methods, before selecting a long-term strategy. A SVA should be:

- **Risk-based**—The approach should be to focus on the most significant security issues in a priority order based on risk. Risk can also be used to judge the adequacy of existing security measures.
- **Structured**—The underlying methodology must be structured to provide a thorough assessment. Some methodologies employ a more rigid structure than others. More flexible structures may be easier to use; however, they generally require more input from subject matter experts. However, all SVA methods identify and use logic to determine how the data considered contributes to risk in terms of affecting the likelihood and/or consequences of potential incidents.
- **Given adequate resources**—Appropriate personnel, time, and financial resources must be allocated to fit the detail level of the assessment.
- **Experience-based**—The frequency and severity of past security related events and the potential for future events should be considered. It is important to understand and account for any actions that have been made to prevent security related events. The SVA should consider the system-specific data and other knowledge about the system that has been acquired by field, operations, and engineering personnel as well as external expertise.
- **Predictive**—A SVA should be investigative in nature, seeking to identify recognized as well as previously unrecognized threats to the facility service and integrity. It should make use of previous security related events, but focus on the potential for future events, including the likelihood of scenarios that may never have happened before.
- **Based on the use of appropriate data**—Some SVA decisions are judgment calls. However, relevant data and particularly data about the system under review should affect the confidence level placed in the decisions.
- **Able to provide for and identify means of feedback**—SVA is an iterative process. Actual field drills, audits, and data collection efforts from both internal and external sources should be used to validate (or invalidate) assumptions made.

2.9 SVA STRENGTHS AND LIMITATIONS

Each of the SVA methods commonly used has its strengths and limitations. Some approaches are well suited to particular applications and decisions, but may not be as helpful in other situations. In selecting or applying SVA methods, there are a number of questions that should be considered. Some of the more significant ones are summarized below.

- Does the scope of the SVA method encompass and identify significant security related events and risks of the facility or along the system? If not, how can the risks that are not included in the SVA method be assessed and integrated in the future?
- Will all data be assessed, as it really exists along the system? Data should be location specific so that additive effects of the various risk variables can be determined. Can the assessment resolution be altered, e.g. station-by-station or mile-by-mile, dependent on the evaluation needs?
- What is the logical structure of variables that are evaluated to provide the qualitative and quantitative results of the SVA? Does this provide for straightforward data assimilation and assessment?
- Does the SVA method use numerical weights and other empirical factors to derive the risk measures and priorities? Are these weights based on the experience of the system, operator, industry, or external sources?
- Do the basic input variables of the SVA method require data that are available to the operator? Do operator data systems and industry data updating procedures provide sufficient support to apply the SVA method effectively? What is the process for updating the SVA data to reflect changes in the system, the infrastructure, and new security related data? How is the input data validated to ensure that the most accurate, up-to-date depiction of the system is reflected in the SVA?
- Does the SVA output provide adequate support for the justification of risk-based decisions? Are the SVA results and output documented adequately to support justification of the decisions made using this output?
- Does the SVA method allow for analysis of the effects of uncertainties in the data, structure, and parameter values on the method output and decisions being supported? What sensitivity or uncertainty analysis is supported by the SVA method?
- Does the SVA method focus exclusively on RMP-based “worst case” events or is it structured to determine “most probable worst case” events that may at times be less severe than postulated in an RMP or include additive effects of adjacent assets to yield consequences more severe than postulated in the RMP?

2.10 RECOMMENDED TIMES FOR CONDUCTING AND REVIEWING THE SVA

The SVA process or SVA methods can be applied at different stages of the overall security assessment and evaluation process. For example, it can be applied to help select, prioritize, and schedule the locations for security assessments. It can also be performed after the security assessment is completed to conduct a more comprehensive SVA that incorporates more accurate information about the facility or pipeline segment.

There are six occasions when the SVA may be required, as illustrated in Figure 2.5.

2.11 VALIDATION AND PRIORITIZATION OF RISKS

Independent of the process used to perform a SVA, the owner/operator must perform a quality control review of the output to ensure that the methodology has produced results consistent with the objectives of the assessment. This can be achieved through a review of the SVA data and results by a knowledgeable and experienced individual or, preferably, by a cross-functional team consisting of a mixture of personnel with skill sets and experience-based knowledge of the systems or segments being reviewed. This validation of the SVA method should be performed to ensure that the method has produced results that make sense to the operator. If the results are not consistent with the operator’s understanding and expectations of system operation and risks, the operator should explore the reasons why and make appropriate adjustments to the method, assumptions, or data. Some additional criteria to evaluate the quality of a SVA are:

- Are the data and analyses handled competently and consistently throughout the system? (Can the logic be readily followed?)
- Is the assessment presented in an organized and useful manner?
- Are all assumptions identified and explained?
- Are major uncertainties identified, e.g., due to missing data?
- Do evidence, analysis, and argument adequately support conclusions and recommendations?

Once the SVA method and process has been validated, the operator has the necessary information to prioritize risks. To determine what risk mitigation actions to take, the operator considers which systems (or segments of systems) have the highest risks and then looks at the reasons the risks are higher for these assets. These risk factors are known as risk drivers since they drive the risk to a higher level for some assets than others do.

2.12 RISK SCREENING

Security issues exist at every facility managed by the petroleum and petrochemical industry, but the threat of intentional acts is likely to be different across the industry. This is captured by the factor known as ‘asset attractiveness’, whereby certain assets are considered to be more attractive to adversaries than others. Based on many reported threat assessments, intelligence reports, and actual events around the world, these factors can be used to evaluate target attractiveness.

It is likely that most facilities have no specific threat history for terrorism. As a result, the assumption must be made that potential malevolent acts are generally credible at each facility and this is then tempered by the site-specific factors. A screening process may contain the following factors:

1. Target attractiveness or target value;
2. Degree of threat;
3. Vulnerability;
4. Potential consequences (casualties, environmental, infrastructure and economic).

These are the same factors as are used for evaluating an individual asset risk, but the difference is that this is done at a generalized facility level for the risk screening instead of at a target asset level. Note that target attractiveness itself includes the factors of consequences and vulnerability. Target attractiveness is an aggregate of factors, which shows the complexity of the process of targeting. Consequences are listed again separately since they have such importance in targeting.

Consequence and target attractiveness are the dominant factors in determining terrorist risk. This is particularly true in the target-rich environment of the United States, where the rare nature of any particular terrorist act vs. the potential number of targets poses a major risk dilemma. Priority should first be given to the consequence ranking, but then consideration should be given to the attractiveness ranking when making assessments. In this way resources can be appropriately applied to assets where they are most likely to be important. This philosophy may be adopted by a company at an enterprise level to help determine both the need to conduct detailed (vs. simpler checklist analyses or audits), and the priority order for the analysis.

Figure 2.5—Recommended Times for Conducting and Reviewing the SVA

1	An initial review of all relevant facilities and assets per a schedule set during the initial planning process
2	When an existing process or operation is proposed to be substantially changed and prior to implementation (revision or rework)
3	When a new process or operation is proposed and prior to implementation (revision or rework)
4	When the threat substantially changes, at the discretion of the manager of the facility (revision or rework)
5	After a significant security incident, at the discretion of the manager of the facility (revision or rework)
6	Periodically to revalidate the SVA (revision or rework)

Chapter 3 Conducting the Security Vulnerability Assessment Methodology

3.1 OVERVIEW OF THE 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 overall 5-step approach of the SVA methodology is described as follows:

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 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.

Once the SVA is completed, there is a need to follow-up on the recommended enhancements to the security countermeasures so they are properly reviewed, tracked, and managed until they are resolved. Resolution may include adoption of the SVA team's recommendations, substitution of other improvements that achieve the same level of risk abatement, or rejection. Rejection of a SVA recommendation and related acceptance of residual risk should be based on valid reasons that are well documented.

This SVA process is summarized in Figure 3.1 and illustrated further in the flowcharts that follow in Figures 3.1a through 3.1c. Section 3.2 of this chapter describes the preparation activities, such as data gathering and forming the SVA team. Sections 3.3 through 3.8 provide details for each step in the SVA methodology. These steps and associated tasks are also summarized in Figure 3.5.

Figure 3.1—Security Vulnerability Assessment Methodology Steps

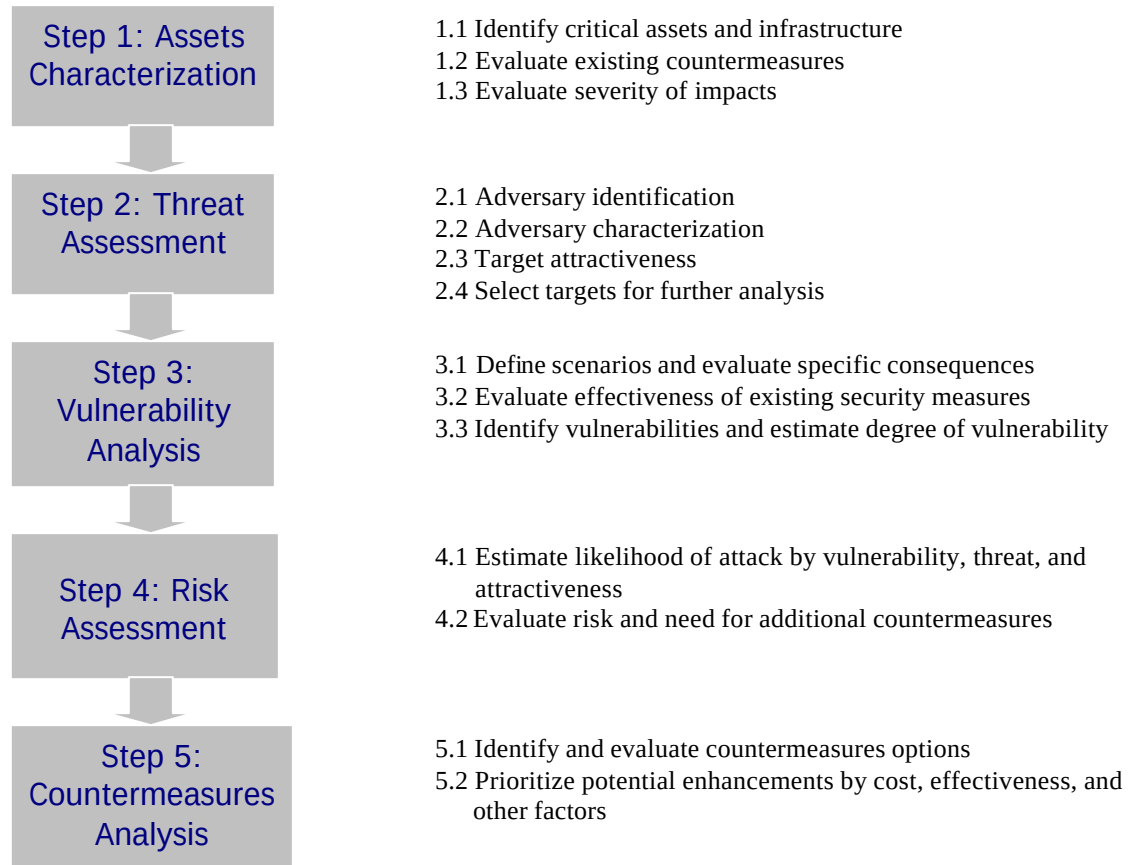


Figure 3.1a—Security Vulnerability Assessment Methodology—Step 1

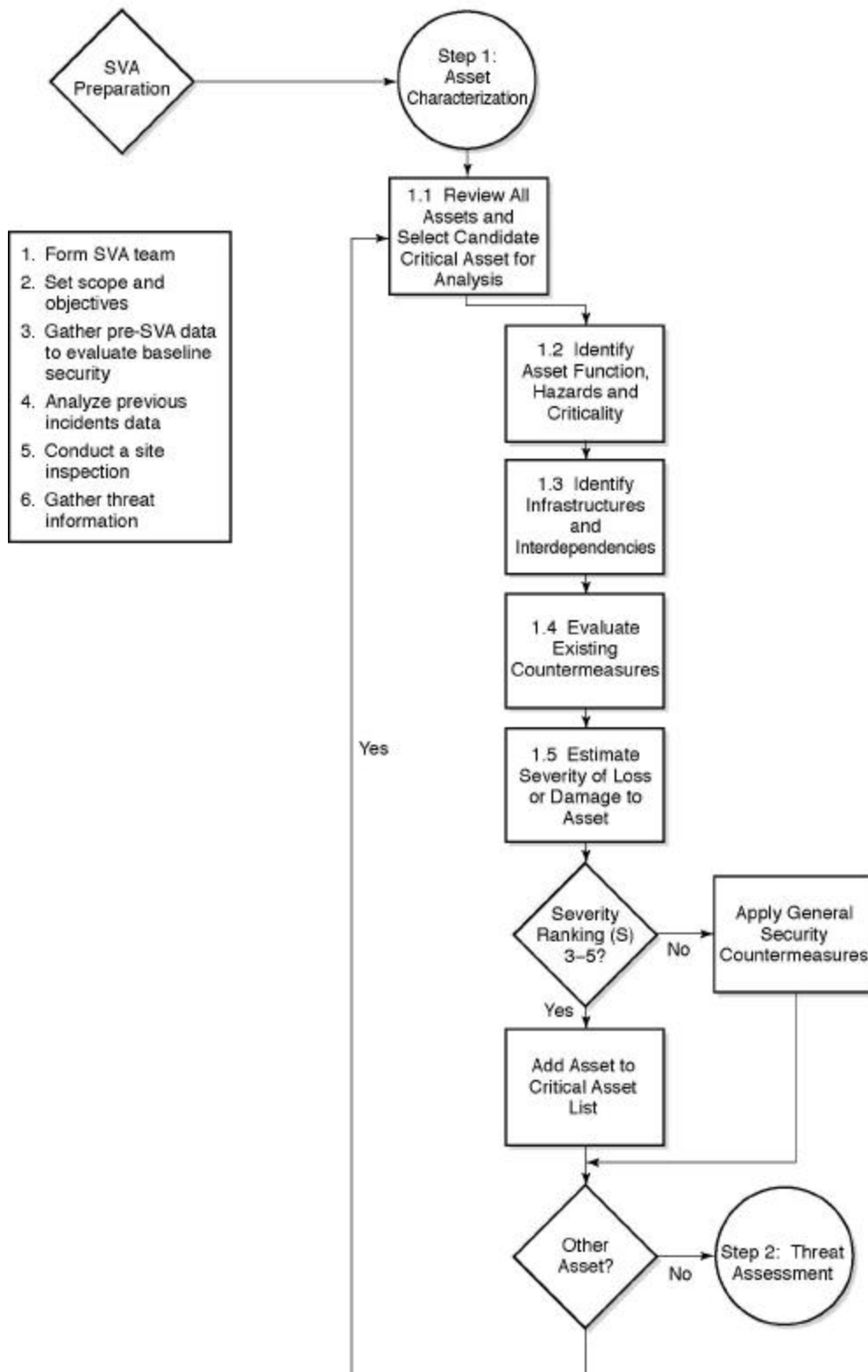


Figure 3.1b—Security Vulnerability Assessment Methodology—Step 2

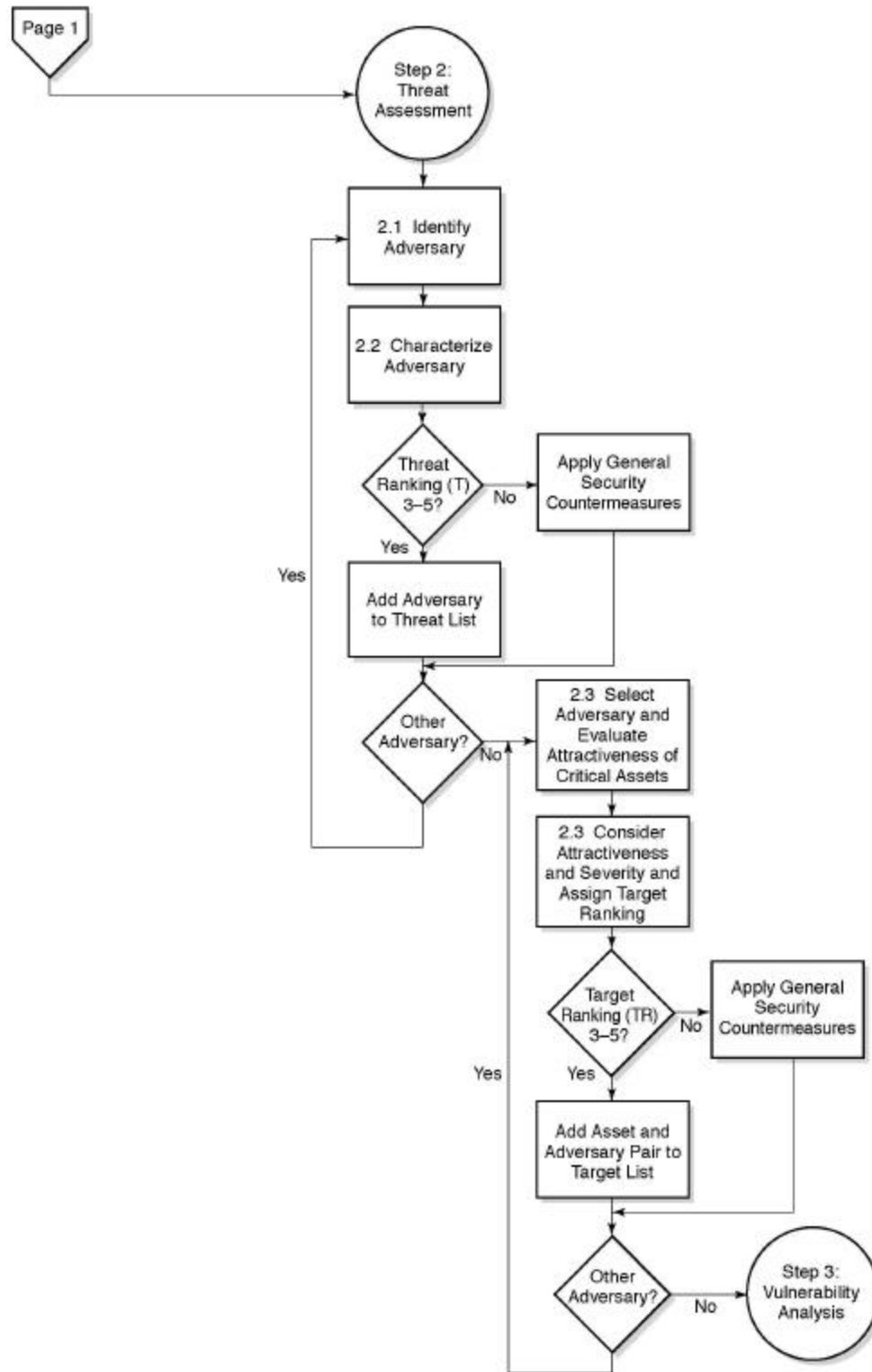
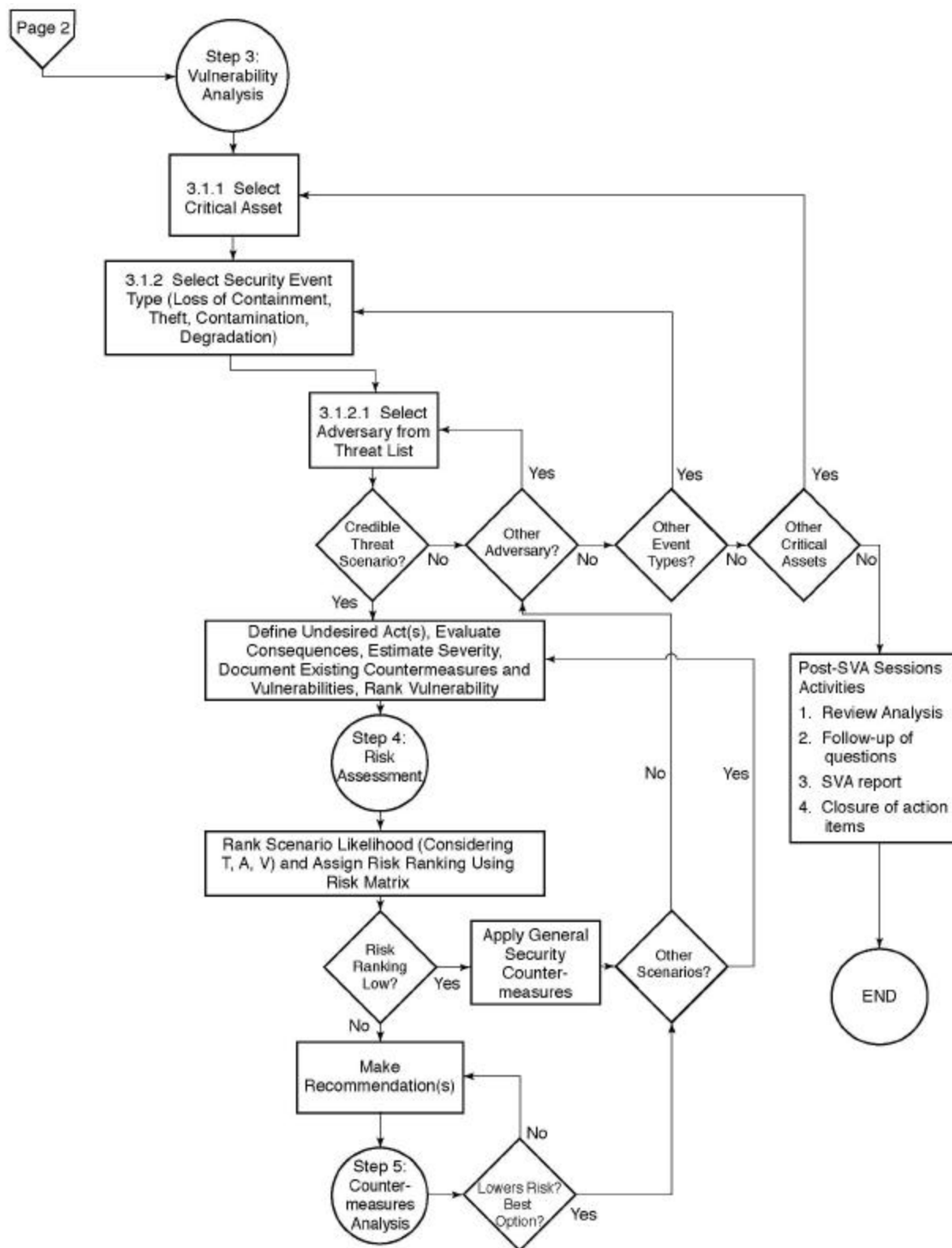


Figure 3.1c—Security Vulnerability Assessment Methodology—Steps 3 – 5



3.2 SVA PREPARATION

3.2.1 Planning for Conducting a SVA

Prior to conducting the SVA team-based sessions, there are a number of activities that must be done to ensure an efficient and accurate analysis. There are many factors in successfully completing a SVA including the following:

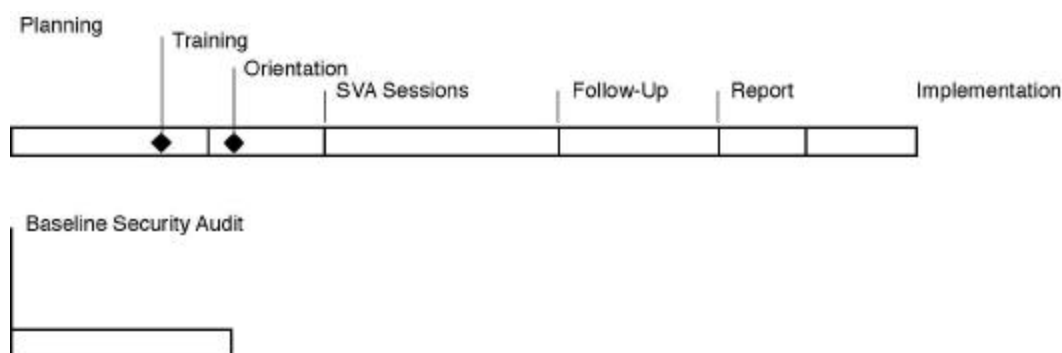
- the activity should be planned well in advance;
- have the full support and authorization by management to proceed;
- the data should be verified and complete;
- the objectives and scope should be concise;
- the team should be knowledgeable of and experienced at the process they are reviewing; and,
- the team leader should be knowledgeable and experienced in the SVA process methodology.

All of the above items are controllable during the planning stage prior to conducting the SVA sessions. Most important for these activities is the determination of SVA specific objectives and scope, and the selection and preparation of the SVA Team.

Prerequisites to conducting the SVA include gathering study data, gathering and analyzing threat information, forming a team, training the team on the method to be used, conducting a baseline security survey, and planning the means of documenting the process.

The typical timeline for conducting a SVA is shown in Figure 3.2.

Figure 3.2—SVA Methodology Timeline



3.2.2 SVA Team

The SVA approach includes the use of a representative group of company experts plus outside experts if needed to identify potential security related events or conditions, the consequences of these events, and the risk reduction activities for the operator's system. These experts draw on the years of experience, practical knowledge, and observations from knowledgeable field operations and maintenance personnel in understanding where the security risks may reside and what can be done to mitigate or ameliorate them.

Such a company group typically consists of representation from: company security, risk management, operations, engineering, safety, environmental, regulatory compliance, logistics/distribution, IT and other team members as required. This group of experts should focus on the vulnerabilities that would enhance the effectiveness of the facility security plan. The primary goal of this group is to capture and build into the SVA method the experience of this diverse group of individual experts so that the SVA process will capture and incorporate information that may not be available in typical operator databases.

If the scope of the SVA includes terrorism and attacks on a process handling flammable or toxic substances, the SVA should be conducted by a team with skills in both the security and process safety areas. This is because the team must evaluate traditional facility security as well as process-safety related vulnerabilities and countermeasures. The final security strategy for protection of the process assets from these events is a combination of security and process safety strategies.

It is expected that a full time 'core' team is primarily responsible, and that they are led by a Team Leader. Other part-time team members, interviewees and guests are used as required for efficiency and completeness. At a minimum, SVA

teams should possess the knowledge and/or skills listed in Figure 3.3. Other skills that should be considered and included, as appropriate, are included as optional or part-time team membership or as guests and persons interviewed.

The SVA Core Team is typically made up of three to five persons, but this is dependent on the number and type of issues to be evaluated and the expertise required to make those judgments. The Team Leader should be knowledgeable and experienced in the SVA approach.

3.2.3 SVA Objectives and Scope

The SVA Team leader should develop an objectives and scope statement for the SVA. This helps to focus the SVA and ensure completeness. An example SVA objectives statement is shown in Figure 3.4.

A work plan should then be developed to conduct the SVA with a goal of achieving the objectives. The work plan needs to include the scope of the effort, which includes which physical or cyber facilities and issues will be addressed.

Given the current focus on the need to evaluate terrorist threats, the key concerns are the intentional (malevolent) misuse of petroleum and hazardous to cause catastrophic consequences. Given this focus, the key events and consequences of interest include the four listed in Figure 3.5. Other events may be included in the scope as determined by the SVA Team, but it is recommended that these four primary security events be addressed first since these are the events that make the petroleum and petrochemical industry unique from other industries.

Figure 3.3—SVA Team Members

<p>The SVA Core Team members should have the following skill sets and experience:</p> <ul style="list-style-type: none"> • Team leader—knowledge of and experience with the SVA methodology; • Security representative—knowledge of facility security procedures, methods and systems; • Safety representative—knowledge of potential process hazards, process safety procedures, methods, and systems of the facility; • Facility representative—knowledge of the design of the facility under study including asset value, function, criticality, and facility procedures; • Operations representative—knowledge of the facility process and equipment operation; • Information systems/Automation representative (for cyber security assessment) —knowledge of information systems technologies and cyber security provisions; knowledge of process control systems.
<p>The SVA Optional/Part-time Team members may include the following skill sets and experience:</p> <ul style="list-style-type: none"> • Security specialist—knowledge of threat assessment, terrorism, weapons, targeting and insurgency/guerilla warfare, or specialized knowledge of detection technologies or other countermeasures available; • Cyber security specialist—knowledge of cyber security practices and technologies; • Subject matter experts on various process or operations details such as process technologies, rotating equipment, distributed control systems, electrical systems, access control systems, etc.; • Process specialist—knowledge of the process design and operations • Management—knowledge of business management practices, goals, budgets, plans, and other management systems.

Figure 3.4—Sample Objectives Statement⁸

To conduct an analysis to identify security hazards, threats, and vulnerabilities facing a fixed facility handling hazardous materials, and to evaluate the countermeasures to provide for the protection of the public, workers, national interests, the environment, and the company.

⁷Ibid, AIChE.

⁸Ibid, AIChE.

Figure 3.5—Security Events of Concern

Security Event Type	Candidate Critical Assets
Loss of Containment, Damage, or Injury	Loss of containment of process hydrocarbons or hazardous chemicals on the plant site from intentional damage of equipment or the malicious release of process materials, which may cause multiple casualties, severe damage, and public or environmental impact. Also included is injury to personnel and the public directly or indirectly
Theft	Hydrocarbon, chemical, or information theft or misuse with the intent to cause severe harm at the facility or offsite
Contamination	Contamination or spoilage of plant products or information to cause worker or public harm on or offsite
Degradation of Assets	Degradation of assets or infrastructure or the business function or value of the facility or the entire company through destructive acts of terrorism.

3.2.4 Data Gathering, Review, and Integration

The objective of this step is to provide a systematic methodology for Owner/Operators to obtain the data needed to manage the security of their facility. Most Owner/Operators will find that many of the data elements suggested here are already being collected. This section provides a systematic review of potentially useful data to support a security plan. However, it should be recognized that all of the data elements in this section are not necessarily applicable to all systems.

The types of data required depend on the types of risks and undesired acts that are anticipated. The operator should consider not only the risks and acts currently suspected in the system, but also consider whether the potential exists for other risks and acts not previously experienced in the system, e.g., bomb blast damage. This section includes lists of many types of data elements. The following discussion is separated into four subsections that address sources of data, identification of data, location of data, and data collection and review.

Appendix A includes a list of potentially useful data that may be needed to conduct a SVA. Appendix B is a checklist of countermeasures that may be used as a data collection form prior to conducting a SVA. Similarly, Appendix C is a checklist for infrastructure and interdependencies that can be used both before and after a SVA for ensuring completeness.

3.2.4.1 Data Sources

The first step in gathering data is to identify the sources of data needed for facility security management. These sources can be divided into four different classes.

1. **Facility and Right of Way Records.** Facility and right of way records or experienced personnel are used to identify the location of the facilities. This information is essential for determining areas and other facilities that either may impact or be impacted by the facility being analyzed and for developing the plans for protecting the facility from security risks. This information is also used to develop the potential impact zones and the relationship of such impact zones to various potentially exposed areas surrounding the facility i.e., population centers, and industrial and government facilities.
2. **System Information.** This information identifies the specific function of the various parts of the process and their importance from a perspective of identifying the security risks and mitigations as well as understanding the alternatives to maintaining the ability of the system to continue operations when a security threat is identified. This information is also important from a perspective of determining those assets and resources available in-house in developing and completing a security plan. Information is also needed on those systems in place, which could support a security plan such as an integrity management program and IT security functions.
3. **Operation Records.** Operating data are used to identify the products transported and the operations as they may pertain to security issues to facilities and pipeline segments which may be impacted by security risks. This information is also needed to prioritize facilities and pipeline segments for security measures to protect the system, e.g., type of product, facility type and location, and volumes transported. Included in operation records data gathering is the need to obtain incident data to capture historical security events.
4. **Outside Support and Regulatory Issues.** This information is needed for each facility or pipeline segment to determine the level of outside support that may be needed and can be expected for the security measures to be employed at each facility or pipeline segment. Data are also needed to understand the expectation for security preparedness and coordination from the regulatory bodies at the government, state, and local levels. Data should also be developed on communication and other infrastructure issues as well as sources of information regarding security threats, e.g., ISACs (Information Sharing and Analysis Centers).

3.2.4.2 Identifying Data Needs

The type and quantity of data to be gathered will depend on the individual facility or pipeline system, the SVA methodology selected, and the decisions that are to be made. The data collection approach will follow the SVA path determined by the initial expert team assembled to identify the data needed for the first pass at SVA. The size of the facility or pipeline system to be evaluated and the resources available may prompt the SVA team to begin their work with an overview or screening assessment of the most critical issues that impact the facility or pipeline system with the intent of highlighting the highest risks. Therefore, the initial data collection effort will only include the limited information necessary to support this SVA. As the SVA process evolves, the scope of the data collection will be expanded to support more detailed assessment of perceived areas of vulnerability.

3.2.4.3 Locating Required Data

Operator data and information are available in different forms and format. They may not all be physically stored and updated at one location based on the current use or need for the information. The first step is to make a list of all data required for security vulnerability assessment and locate the data. The data and information sources may include:

- Facility plot plans, equipment layouts and area maps
- Process and Instrument Drawings (P&IDs)
- Pipeline alignment drawings
- Existing company standards and security best practices
- Product throughput and product parameters
- Emergency response procedures
- Company personnel interviews
- LEPC (Local Emergency Planning Commission) response plans
- Police agency response plans
- Historical security incident reviews
- Support infrastructure reviews

3.2.4.4 Data Collection and Review

Every effort should be made to collect good quality data. When data of suspect quality or consistency are encountered, such data should be flagged so that during the assessment process, appropriate confidence interval weightings can be developed to account for these concerns.

In the event that the SVA approach needs input data that are not readily available, the operator should flag the absence of information. The SVA team can then discuss the necessity and urgency of collecting the missing information

3.2.5 Analyzing Previous Incidents Data

Any previous security incidents relevant to the security vulnerability assessment may provide valuable insights to potential vulnerabilities and trends. These events from the site and, as available, from other historical records and references, should be considered in the analysis. This may include crime statistics, case histories, or intelligence relevant to facility.

3.2.6 Conducting a Site Inspection

Prior to conducting the SVA sessions, it is necessary for the team to conduct a site inspection to visualize the facility and to gain valuable insights to the layout, lighting, neighboring area conditions, and other facts that may help understand the facility and identify vulnerabilities. The list of data requirements in Appendix A and the checklist in Appendix B may be referenced for this purpose.

3.2.7 Gathering Threat Information

The team should gather and analyze relevant company and industry or government-provided threat information, such as that available from the Energy ISAC, DHS, FBI, or other local law enforcement agency.

3.3 STEP 1: ASSETS CHARACTERIZATION

Characterization of the facility is a step whereby the facility assets and hazards are identified, and the potential consequences of damage or theft to those assets is analyzed. The focus is on processes which may contain petroleum or hazardous chemicals and key assets, with an emphasis on possible public impacts. The Asset Attractiveness, based on

these and other factors, is included in the facility characterization. These two factors (severity of the consequences and asset attractiveness) are used to screen the facility assets into those that require only general vs. those that require more specific security countermeasures.

The team produces a list of candidate critical assets that need to be considered in the analysis. Attachment 1—Step 1: Critical Assets/Criticality Form is helpful in developing and documenting the list of critical assets. The assets may be processes, operations, personnel, or any other asset as described in Chapter 3.

Figure 3.6 below summarizes the key steps and tasks required for Step 1.

Step 1.1—Identify Critical Assets

The SVA Team should identify critical assets for the site being studied. The focus is on petroleum or chemical process assets, but any asset may be considered. For example, the process control system may be designated as critical, since protection of it from physical and cyber attack may be important to prevent a catastrophic release or other security event of concern. Figure 3.7 is an example list of specific assets that may be designated as critical at any given site. Assets include the full range of both material and non-material aspects that enable a facility to operate.

Figure 3.6—Description of Step 1 and Substeps

Step	Task
Step 1: Assets Characterization	
1.1 Identify critical assets	Identify critical assets of the facility including people, equipment, systems, chemicals, products, and information.
1.2 Identify critical functions	Identify the critical functions of the facility and determine which assets perform or support the critical functions.
1.3 Identify critical infrastructures and interdependencies	Identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset.
1.4 Evaluate existing countermeasures	Identify what protects and supports the critical functions and assets. Identify the relevant layers of existing security systems including physical, cyber, operational, administrative, and business continuity planning, and the process safety systems that protect each asset.
1.5 Evaluate impacts	Evaluate the hazards and consequences or impacts to the assets and the critical functions of the facility from the disruption, damage, or loss of each of the critical assets or functions.
1.6 Select targets for further analysis	Develop a target list of critical functions and assets for further study.

Figure 3.7—Example Candidate Critical Assets

Security Event Type	Candidate Critical Assets
Loss of Containment, Damage, or Injury	<ul style="list-style-type: none"> • Process equipment handling petroleum and hazardous materials including processes, pipelines, storage tanks • Marine vessels and facilities, pipelines, other transportation systems • Employees, contractors, visitors in high concentrations
Theft	<ul style="list-style-type: none"> • Hydrocarbons or chemicals processed, stored, manufactured, or transported • Metering stations, process control and inventory management systems • Critical business information from telecommunications and information management systems including Internet accessible assets
Contamination	<ul style="list-style-type: none"> • Raw material, intermediates, catalysts, products, in processes, storage tanks, pipelines • Critical business or process data
Degradation of Assets	<ul style="list-style-type: none"> • Processes containing petroleum or hazardous chemicals • Business image and community reputation • Utilities (electric power, steam, water, natural gas, specialty gases) • Telecommunications Systems • Business systems

The following information should be reviewed by the SVA Team as appropriate for determination of applicability as critical assets:

- Any applicable regulatory lists of highly hazardous chemicals, such as the Clean Air Act 112(r) list of flammable and toxic substances for the EPA Risk Management Program (RMP) 40 *CFR* Part 68 or the OSHA Process Safety Management (PSM) 29 *CFR* 1910.119 list of highly hazardous chemicals;
- Inhalation poisons or other chemicals that may be of interest to adversaries;
- Large and small scale chemical weapons precursors as based on the following lists:
 - Chemical Weapons Convention list;
 - FBI Community Outreach Program (FBI List) for Weapons of Mass Destruction materials and precursors;
 - The Australia Group list of chemical and biological weapons
- Material destined for the food, nutrition, cosmetic or pharmaceutical chains;
- Chemicals which are susceptible to reactive chemistry.

Owner/Operators may wish to consider other categories of chemicals that may cause losses or injuries that meet the objectives and scope of the analysis. These may include other flammables, critically important substances to the process, explosives, radioactive materials, or other chemicals of concern.

In addition, the following personnel, equipment and information may be determined to be critical:

- Process equipment
- Critical data
- Process control systems
- Personnel
- Critical infrastructure and support utilities

Step 1.2—Identify Critical Functions

The SVA Team should identify the critical functions of the facility and determine which assets perform or support the critical functions. For example, the steam power plant of a refinery may be critical since it is the sole source of steam supply to the refinery.

Step 1.3—Identify Critical Infrastructures and Interdependencies

The SVA team should identify the critical internal and external infrastructures and their interdependencies (e.g., electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and SCADA systems) that support the critical operations of each asset. For example, the electrical substation may be the sole electrical supply to the plant, or a supplier delivers raw material to the facility via a single pipeline. Appendix C, Interdependencies and Infrastructure Checklist, can be used to identify and analyze these issues. Note that some of these issues may be beyond the control of the owner/operator, but it is necessary to understand the dependencies and interdependencies of the facility, and the result of loss of these systems on the process.

Step 1.4—Evaluate Existing Countermeasures

The SVA team identifies and documents the existing security and process safety layers of protection. This may include physical security, cyber security, administrative controls, and other safeguards. During this step the objective is to gather information on the types of strategies used, their design basis, and their completeness and general effectiveness. A pre-SVA survey is helpful to gather this information. The data will be made available to the SVA team for them to form their opinions on the adequacy of the existing security safeguards during Step 3: Vulnerability Analysis and Step 5: Countermeasures Analysis.

Appendix B—Countermeasures Survey Form can be used to gather information on the presence and status of existing safeguards or another form may be more suitable. Existing records and documentation on security and process safety systems, as well as on the critical assets themselves, can be referenced rather than repeated in another form of documentation.

The objective of the physical security portion of the survey is to identify measures that protect the entire facility and/or each critical asset of the facility, and to determine the effectiveness of the protection. Appendix B contains checklists that may be used to conduct the physical security portion of the survey.

Note that the infrastructure interdependencies portion of the survey will identify infrastructures that support the facility and/or its critical assets (e.g., electric power, water, and telecommunications). A physical security review of these vital infrastructures should also be conducted.

Step 1.5—Evaluate Impacts

The Impacts Analysis step includes both the determination of the hazards of the asset being compromised as well as the specific consequences of a loss. The SVA team should consider relevant chemical use and hazard information, as well as information about the facility. The intent is to develop a list of target assets that require further analysis partly based on the degree of hazard and consequences. Particular consideration should be given to the hazards of fire, explosion, toxic release, radioactive exposure, and environmental contamination.

The consequences are analyzed to understand their possible significance. The Appendix A—Attachment 1—Step 1: Critical Assets/Criticality Form is useful to document the general consequences for each asset. The consequences may be generally described but consideration should be given to those listed in Figure 3.8.

Figure 3.8—Possible Consequences of Security Events

Public fatalities or injuries
Site personnel fatalities or injuries
Large-scale disruption to the national economy, public or private operations
Large-scale disruption to company operations
Large-scale environmental damage
Large-scale financial loss
Loss of critical data
Loss of reputation or business viability

The consequence analysis is done in a general manner. If the security event involves a toxic or flammable release to the atmosphere, the EPA RMP offsite consequence analysis guidance can be used as a starting point. If it is credible to involve more than the largest single vessel containing the hazardous material in a single incident, the security event may be larger than the typical EPA RMP worst-case analysis.

A risk ranking scale can be used to rank the degree of severity. Figure 3.9 illustrates a set of consequence definitions based on four categories of events—A. Fatalities and injuries; B. Environmental impacts; C. Property damage; and D. Business interruption.

Figure 3.9—Example Definitions of Consequences of the Event

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

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 off-site 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.

Step 1.6—Select Targets for Further Analysis

For each asset identified, the criticality of each asset must be understood. This is a function of the value of the asset, the hazards of the asset, and the consequences if the asset was damaged, stolen, or misused. For hazardous chemicals, consideration may include toxic exposure to workers or the community, or potential for the misuse of the chemical to produce a weapon or the physical properties of the chemical to contaminate a public resource.

The SVA Team develops a Target Asset List which is a list of the assets associated with the site being studied that are more likely to be attractive targets, based on the complete list of assets and the identified consequences and targeting issues identified in the previous steps. During Step 3: Vulnerability Analysis, the Target Asset List will be generally paired with specific threats and evaluated against the potential types of attack that could occur.

The SVA methodology uses ranking systems that are based on a scale of 1 –s 5 where 1 is the lowest value and 5 is the highest value. Based on the consequence ranking and criticality of the asset, the asset is tentatively designated a candidate critical target asset. The attractiveness of the asset will later be used for further screening of important assets.

3.4 STEP 2: THREAT ASSESSMENT

The threat assessment step involves the substeps shown in Figure 3.10.

Step 2.1—Adversary Identification

The next step is to identify specific classes of adversaries that may perpetrate the security-related events. The adversary characterization sub-step involves developing as complete an understanding as is possible of the adversary's history, capabilities and intent. A threat matrix is developed to generally pair the assets with each adversary class as shown in Attachment 1—Step 2: Threat Assessment Form.

Figure 3.10—Description of Step 2 and Substeps

Step	Task
Step 2: Threat Assessment	
2.1 Adversary identification	Evaluate threat information and identify threat categories and potential adversaries. Identify general threat categories. Consider threats posed by insiders, external agents (outsiders), and collusion between insiders and outsiders.
2.2 Adversary characterization	Evaluate each adversary and provide an overall threat assessment/ ranking for each adversary using known or available information. Consider such factors as the general nature/history of threat; specific threat experience/history to the facility/operation; known capabilities/methods/weapons; potential actions, intent/ motivation of adversary.
2.3 Analyze target attractiveness	Conduct an evaluation of target (from assets identified in Step 1) attractiveness from the adversary perspective.

Depending on the threat, the analyst can determine the types of potential attacks and, if specific information is available (intelligence) on potential targets and the likelihood of an attack, specific countermeasures may be taken. Information may be too vague to be useful, but SVA Teams should seek available information from Federal, State, and Local law enforcement officials in analyzing threats. Absent specific threat information, the SVA can still be applied based on assuming general capabilities and characteristics of typical hypothetical adversaries.

Threat assessment is an important part of a security management system, especially in light of the emergence of international terrorism in the United States. There is a need for understanding the threats facing the industry and any given facility or operation to properly respond to those threats. This section describes a threat assessment approach as part of the security management process. Later in Section 3.0 the use of the threat assessment in the SVA process will be more fully explained.

A threat assessment is used to evaluate the likelihood of adversary activity against a given asset or group of assets. It is a decision support tool that helps to establish and prioritize security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability, intention, and impact of an attack.

Threat assessment is a process that must be systematically done and kept current to be useful. The determination of these threats posed by different adversaries leads to the recognition of vulnerabilities and to the evaluation of required countermeasures to manage the threats. Without a design basis threat or situation specific threat in mind, a company cannot effectively develop a cost-effective security management system.

In characterizing the threat to a facility or a particular asset for a facility, a company should examine the historical record of security events and obtains available general and location-specific threat information from government organizations and other sources. It should then evaluate these threats in terms of company assets that represent likely targets.

Some threats are assumed continuous, whereas others are assumed to be variable. As such, this guidance follows the Department of Homeland Security's Homeland Security Advisory System (HSAS) and the U.S.C.G. Maritime Security (MARSEC) security levels for management of varying threat levels to the industry. The threat assessment determines the estimated general threat level, which varies as situations develop. Depending on the threat level, different security measures over baseline measures will likely be necessary.

While threat assessments are key decision support tools, it should be recognized that, even if updated often, threat assessments might not adequately capture emerging threats posed by some adversary groups. No matter how much we know about potential threats, we will never know that we have identified every threat or that we have complete information even about the threats of which we are aware. Consequently, a threat assessment must be accompanied by a vulnerability assessment to provide better assurance of preparedness for a terrorist or other adversary attack.

Intelligence and law enforcement agencies assess the foreign and domestic terrorist threats to the United States. The U.S. intelligence community—which includes the Central Intelligence Agency, the Defense Intelligence Agency, and the State Department's Bureau of Intelligence and Research, among others—monitors the foreign-origin terrorist threat to the United States. The FBI gathers information and assesses the threat posed by domestic sources of terrorism.

Threat information gathered by both the intelligence and law enforcement communities can be used to develop a company-specific threat assessment. A company attempts to identify threats in order to decide how to manage risk in a cost-effective manner. All companies are exposed to a multitude of threats, including terrorism or other forms of threat.

A threat assessment can take different forms, but the key components are:

1. Identification of known and potential adversaries;
2. Recognition and analysis of their intentions, motivation, operating history, methods, weapons, strengths, weaknesses, and intelligence capabilities;
3. Assessment of the threat posed by the adversary factors mentioned above against each asset, and the assignment of an overall criticality ranking for each adversary.

Threats need to be considered from both insiders and outsiders, or a combination of those adversaries working in collusion. Insiders are defined as those individuals who normally have authorized access to the asset. They pose a particularly difficult threat, due to the possibility for deceit, deception, training, knowledge of the facilities, and unsupervised access to critical information and assets.

The threat categories to be considered are those that include intent and capability of causing major catastrophic harm to the facilities and to the public or environment. Typical adversaries that may be included in a SVA are: international terrorists, domestic terrorists (including disgruntled individuals/'lone wolf' sympathizers), disgruntled employees, or extreme activists.

All companies are encouraged to discuss threats with local and Federal law enforcement officials, and to maintain networking with fellow industrial groups to improve the quality of applicable threat information.

The threat assessment is not necessarily based on perfect information. In fact, for most facilities, the best available information is vague or nonspecific to the facility. A particularly frustrating part of the analysis can be the absence of site-specific information on threats. A suggested approach is to make an assumption that international terrorism is possible at every facility that has adequate attractiveness to that threat. Site-specific information adjusts the generic average rankings accordingly.

To be effective, threat assessment must be considered a dynamic process, whereby the threats are continuously evaluated for change. During any given SVA exercise, the threat assessment is referred to for guidance on general or specific threats facing the assets. At that time the company's threat assessment should be referred to and possibly updated as required given additional information and analysis of vulnerabilities.

Figure 3.11 includes a five level ranking system for defining threats against an asset.

Step 2.2—Adversary Characterization

Insiders, outsiders or a combination of the two may perpetrate an attack. Insiders are personnel that have routine, unescorted access within the facility. Outsiders do not. Collusion between the two may be the result of monetary gain (criminal insider/terrorist outsider), ideological sympathy, or coercion.

The adversary characterization will assist in evaluating the attack issues associated with insider, outsider, and colluding adversary threats. The SVA team should consider each type of adversary identified as credible, and generally define their level of capabilities, motivation, and likelihood of threat.

Step 2.3—Analyze Target Attractiveness

The team assigns the target attractiveness ranking. To facilitate this use Attachment 1—Threat Assessment: Target Attractiveness Form can be used.

The attractiveness of the target to the adversary is a key factor in determining the likelihood of an attack. Examples of issues that may be addressed here include:

- Proximity to a symbolic or iconic target, such as a national landmark
- Unusually high corporate profile among possible terrorists, such as a major defense contractor
- Any other variable not addressed elsewhere, when the SVA Team agrees it has an impact on the site's value as a target or on the potential consequences of an attack.

The SVA Team should use the best judgment of its subject matter experts to assess attractiveness. This is a subjective process as are all vulnerability assessments whether qualitative or quantitative in nature.

Each asset is analyzed to determine the factors that might make it a more or less attractive target to the adversary. Attractiveness is used to assess likelihood of the asset being involved in an incident.

Target Attractiveness is an assessment of the target's value from the adversary's perspective, which is one factor used as a surrogate measure for likelihood of attack. Note that target attractiveness itself includes the other factors of consequences and difficulty of attack/vulnerability. Target attractiveness is an aggregate of factors, which shows the complexity of the process of targeting and anti-terrorism efforts. Arguably target attractiveness is the dominant factor in determining terrorist risk. This is particularly true in the target-rich environment of the United States, where the rare nature of any particular terrorist act vs. the potential number of targets poses a major risk assessment dilemma.

The attractiveness of assets varies with the adversary threat including their motivation, intent, and capabilities. For example, the threat posed by an international terrorist and the assets they might be interested in could greatly vary from the threat and assets of interest to a violent activist or environmental extremist.

Figure 3.12 shows the factors that should be evaluated when evaluating target attractiveness for terrorism. The team can use these factors and rank each asset against each adversary by the scale shown in Figure 3.13. Other adversaries may be interested in other factors, and the user of the SVA is encouraged to understand the relevant factors and substitute them for those in Figure 3.12 as applicable.

3.5 SVA STEP 3: VULNERABILITY ANALYSIS

The Vulnerability Analysis step involves three steps, as shown in Figure 3.14. Once the SVA Team has determined how an event can be induced, it should determine how an adversary could make it occur. There are two schools of thought on methodology: the scenario-based approach and the asset-based approach. Both approaches are identical in the beginning, but differ in the degree of detailed analysis of threat scenarios and specific countermeasures applied to a given scenario. The assets are identified, and the consequences and target attractiveness are analyzed as per Step 2, for both approaches. Both approaches result in a set of annotated potential targets, and both approaches may be equally successful at evaluating security vulnerabilities and determining required protection.

Figure 3.11—Threat Rating Criteria

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.

Figure 3.12—Target Attractiveness Factors (for Terrorism)

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
• Recognition of the target

Figure 3.13—Attractiveness Factors Ranking Definitions (A)

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

Figure 3.14—Description of Step 3 and Substeps

Step	Task
Step 3: Vulnerability Analysis	
3.1 Define scenarios and evaluate specific consequences	Use scenario-analysis and/or use asset-based analysis to document the adversary's potential actions against an asset.
3.2 Evaluate effectiveness of existing security measures	Identify the existing measures intended to protect the critical assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary.
3.3 Identify vulnerabilities and estimate degree of vulnerability	Identify the potential vulnerabilities of each critical asset to applicable threats or adversaries. Estimate the degree of vulnerability of each critical asset for each threat-related undesirable event or incident and thus each applicable threat or adversary.

Step 3.1—Define Scenarios and Evaluate Specific Consequences

Each asset in the list of critical target assets from Step 2 is reviewed in light of the threat assessment, and the relevant threats and assets are paired in a matrix or other form of analysis, as shown in Attachment 1—Steps 3 – 5—Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form. The importance of this step is to develop a design basis threat statement for each facility.

Once the SVA Team has determined how a malevolent event can be induced, it should determine how an adversary could execute the act.

The action in the Scenario-based approach follow the SVA method as outlined in Chapter 3. To establish an understanding of risk, scenarios can be assessed in terms of the severity of consequences and the likelihood of occurrence of security events. These are qualitative analyses based on the judgment and deliberation of knowledgeable team members.

Step 3.2—Evaluate Effectiveness of Existing Security Measures

The SVA Team will identify the existing measures intended to protect the critical assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat or adversary.

Step 3.3—Identify Vulnerabilities and Estimate Degree of Vulnerability

Vulnerability is any weakness that can be exploited by an adversary to gain unauthorized access and the 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.

For each asset, the vulnerability or difficulty of attack is considered using the definitions shown in Figure 3.15.

The Scenario-based approach is identical to the Asset-based approach in the beginning, but differs in the degree of detailed analysis of threat scenarios. The scenario-based approach uses a more detailed analysis strategy and brainstorms a list of scenarios to understand how the undesired event might be accomplished. The scenario-based approach begins with an onsite inspection and interviews to gather specific information for the SVA Team to consider.

The following is a description of the approach and an explanation of the contents of each column of the worksheet in Attachment 1—Steps 3 – 5 Scenario Based Vulnerability Worksheet/Risk Ranking/Countermeasures Form.

Figure 3.15—Vulnerability Rating Criteria

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.

The SVA Team devises a scenario based on their perspective of the consequences that may result from undesired security events given a postulated threat for a given asset. This is described as an event sequence including the specific malicious act or cause and the potential consequences, while considering the challenge to the existing countermeasures. It is conservatively assumed that the existing countermeasures are exceeded or fail in order to achieve the most serious consequences, in order to understand the hazard. When considering the risk, the existing countermeasures need to be assessed as to their integrity, reliability, and ability to deter, detect, and delay.

In this column the type of malicious act is recorded. As described in Chapter 2, the four types of security events included in the objectives of a SVA at a minimum include:

1. Theft/Diversion of material for subsequent use as a weapon or a component of a weapon
2. Causing the deliberate loss of containment of a chemical present at the facility
3. Contamination of a chemical, tampering with a product, or sabotage of a system
4. An act causing degradation of assets, infrastructure, business and/or value of a company or an industry.

Given the information collected in Steps 1 – 3 regarding the site's key target assets, the attractiveness of these targets, and the existing layers and rings of protection, a description of the initiating event of a malicious act scenario may be entered into the Undesired Event column. The SVA team brainstorms the vulnerabilities based on the information collected in Steps 1 – 3. The SVA team should brainstorm vulnerabilities for all of the malicious act types that are applicable at a minimum. Other scenarios may be developed as appropriate.

Completing the Worksheet

The next step is for the team to evaluate scenarios concerning each asset/threat pairing as appropriate. The fields in the worksheet are completed as follows:

1. **Asset:** The asset under consideration is documented. The team selects from the targeted list of assets and considers the scenarios for each asset in turn based on priority.
2. **Security Event Type:** This column is used to describe the general type of malicious act under consideration. At a minimum, the four types of acts previously mentioned should be considered as applicable.
3. **Threat Category:** The category of adversary including terrorist, activist, disgruntled employee, etc.
4. **Type:** The type of adversary category whether (I) – Insider, (E) – External, or (C) – Colluded threat.
5. **Undesired Act:** A description of the sequence of events that would have to occur to breach the existing security measures is described in this column.
6. **Consequences:** Consequences of the event are analyzed and entered into the Consequence column of the worksheet. The consequences should be conservatively estimated given the intent of the adversary is to maximize their gain.
It is recognized that the severity of an individual event may vary considerably, so SVA teams are encouraged to understand the expected consequence of a successful attack or security breach.
7. **Consequences Ranking:** Severity of the Consequences on a scale of 1 – 5 as shown in Figure 3.8. The severity rankings are assigned based on a conservative assumption of a successful attack.

8. **Existing Countermeasures:** The existing security countermeasures that relate to detecting, delaying, or deterring the adversaries from exploiting the vulnerabilities may be listed in this column. The countermeasures have to be functional (i.e., not bypassed or removed) and sufficiently maintained as prescribed (i.e., their ongoing integrity can be assumed to be as designed) for credit as a countermeasure.
9. **Vulnerability:** The specific countermeasures that would need to be circumvented or failed should be identified.
10. **Vulnerability Ranking:** The degree of vulnerability to the scenario rated on a scale of 1 – 5 as shown in Figure 3.15.
11. **L(ikelihood):** The likelihood of the security event is assigned a qualitative ranking in the likelihood column. The likelihood rankings are generally assigned based on the likelihood associated with the entire scenario, assuming that all countermeasures are functioning as designed/intended. Likelihood is a team decision and is assigned from the Likelihood scale based on the factors of Vulnerability, Attractiveness, and Threat for the particular scenario considered.
12. **R(isk):** The severity and likelihood rankings are combined in a relational manner to yield a risk ranking. The development of a risk-ranking scheme, including the risk ranking values is described in Step 4.
13. **New Countermeasures:** The recommendations for improved countermeasures that are developed are recorded in the New Countermeasures column.

3.6 STEP 4: RISK ANALYSIS/RANKING

In either the Asset-based or the Scenario-based approach to Vulnerability Analysis, the next step is to determine the level of risk of the adversary exploiting the asset given the existing security countermeasures. Figure 3.16 lists the substeps.

The scenarios are risk-ranked by the SVA Team based on a simple scale of 1 – 5. The risk matrix shown in Figure 3.17 could be used to plot each scenario based on its likelihood and consequences. The intent is to categorize the assets into discrete levels of risk so that appropriate countermeasures can be applied to each situation.

Note: For this matrix, a Risk Ranking of “5 x 5” represents the highest severity and highest likelihood possible.

3.7 STEP 5: IDENTIFY COUNTERMEASURES:

A Countermeasures Analysis identifies shortfalls between the existing security and the desirable security where additional recommendations may be justified to reduce risk. In assessing the need for additional countermeasures, the team should ensure each scenario has the following countermeasures strategies employed:

- **DETER** an attack if possible
- **DETECT** an attack if it occurs
- **DELAY** the attacker until appropriate authorities can intervene
- **RESPOND** to neutralize the adversary, to evacuate, shelter in place, call local authorities, control a release, or other actions.

The SVA Team evaluates the merits of possible additional countermeasures by listing them and estimating their net effect on the lowering of the likelihood or severity of the attack. The team attempts to lower the risk to the corporate standard.

Figure 3.16—Description of Step 4 and Substeps

Step	Task
Step 4: Risk Assessment	
4.1 Estimate risk of successful attack	As a function of consequence and probability of occurrence, determine the relative degree of risk to the facility in terms of the expected effect on each critical asset (a function of the consequences or impacts to the critical functions of the facility from the disruption or loss of the critical asset, as evaluated in Step 1) and the likelihood of a successful attack (a function of the threat or adversary, as evaluated in Step 2, and the degree of vulnerability of the asset, as evaluated in Step 3).
4.2 Prioritize risks	Prioritize the risks based on the relative degrees of risk and the likelihoods of successful attacks.

Figure 3.17—Risk Ranking Matrix

L I K E L I H O O D	SEVERITY				
	5	4	3	2	1
	5	High	High	High	Med
	4	High	High	Med	Med
	3	High	Med	Med	Low
	2	Med	Med	Low	Low
	1	Med	Low	Low	Low

Figure 3.18—Description of Step 5 and Substeps

Step	Task
Step 5: Countermeasures Analysis	
5.1 Identify and evaluate enhanced countermeasures options	Identify countermeasures options to further reduce the vulnerabilities and thus the risks while considering such factors as: <ul style="list-style-type: none"> • Reduced probability of successful attack • The degree of risk reduction provided by the options • The reliability and maintainability of the options • The capabilities and effectiveness of these mitigation options • The costs of the mitigation options • The feasibility of the options Rerank to evaluate effectiveness.
5.2 Prioritize potential enhancements	Prioritize the alternatives for implementing the various options and prepare recommendations for decision makers

3.8 FOLLOW-UP TO THE SVA

The outcome of the SVA is:

- the identification of security vulnerabilities;
- a set of recommendations (if necessary) to reduce risk to an acceptable level.

The SVA results should include a written report that documents:

- The date of the study;
- The study team members, their roles and expertise and experience;
- A description of the scope and objectives of the study;
- A description of or reference to the SVA methodology used for the study;
- The critical assets identified and their hazards and consequences;
- The security vulnerabilities of the facility;
- The existing countermeasures;
- A set of prioritized recommendations to reduce risk.

Once the report is released, it is necessary for a resolution management system to resolve issues in a timely manner and to document the actual resolution of each recommended action.

Attachment 1—Example SVA Methodology Forms

The following four forms can be used to document the SVA results. Blank forms are provided, along with a sample of how each form is to be completed. Other forms of documentation that meet the intent of the SVA guidance can be used.

Step 1: Critical Assets/Criticality Form		
Facility Name:		
Critical Assets Form		
Critical Assets	Criticality/Hazards	Asset Severity Ranking
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		

Step 2: Threat Assessment Form								
General Adversary Type	Source	General Threat History	Site Specific Threat History	Potential Actions	Adversary Capability	Adversary Motivation/ Intent	Overall Assessment	Threat Ranking
1. International Terrorists								
2. Domestic Terrorists								
3. Domestic Disgruntled Employee or Contractor								
4. Domestic Activists								

Step 2: Attractiveness/Target Ranking Form									
Facility Name:									
Critical Assets	Function/Hazards/ Criticality	Asset Severity Ranking	Asset Attractiveness						
			Foreign/Domestic Attractiveness Rationale	A1	Employee/ Contractor Attractiveness Rationale	A2	Activist Attractiveness Rationale	A3	TR
1.									
2.									
3.									
4.									
5.									
6.									

Step 3 – 5: Vulnerability Analysis/Risk Ranking/Countermeasures Form**Facility Name:****Critical Assets:****Attractiveness:**

Security Event Type	Threat Category	Type	Undesired Act	Consequences	S	Existing Countermeasures	Vulnerability	V	L	R	New Countermeasures

Glossary of Terms¹²

Adversary: Any individual, group, organization, or government that conducts activities, or has the intention and capability to conduct activities detrimental to critical assets. An adversary could include intelligence services of host nations, or third party nations, political and terrorist groups, criminals, rogue employees, and private interests. Adversaries can include site insiders, site outsiders, or the two acting in collusion.

Alert levels: Describes a progressive, qualitative measure of the likelihood of terrorist actions, from negligible to imminent, based on government or company intelligence information. Different security measures may be implemented at each alert level based on the level of threat to the facility.

Asset: An asset is any person, environment, facility, material, information, business reputation, or activity that has a positive value to an owner. The asset may have value to an adversary, as well as an owner, although the nature and magnitude of those values may differ. Assets in the SVA include the community and the environment surrounding the site.

Asset category: Assets may be categorized in many ways. Among these are:

- People
- Hazardous materials (used or produced)
- Information
- Environment
- Equipment
- Facilities
- Activities/Operations
- Company reputation

Benefit: Amount of expected risk reduction based on the overall effectiveness of countermeasures with respect to the assessed vulnerabilities.

Capability: When assessing the capability of an adversary, two distinct categories need to be considered. The first is the capability to obtain, damage, or destroy the asset. The second is the adversary's capability to use the asset to achieve their objectives once the asset is obtained, damaged, or destroyed.

Checklist: A list of items developed on the basis of past experience that is intended as a guide to assist in applying a standard level of care for the subject activity and to assist in completing the activity in as thorough a manner.

Consequences: The amount of loss or damage that can be expected, or may be expected from a successful attack against an asset. Loss may be monetary but may also include political, morale, operational effectiveness, or other impacts. The impacts of security events, which should involve those that are extremely severe. Some examples of relevant consequences in a SVA include fatality to member(s) of the public, fatality to company personnel, injuries to member(s) of the public, injuries to company personnel, large-scale disruption to public or private operations, large-scale disruption to company operations, large-scale environmental damage, large-scale financial loss, loss of critical data, and loss of reputation.

Cost: Includes tangible items such as money and equipment as well as the operational costs associated with the implementation of countermeasures. There are also intangible costs such as lost productivity, morale considerations, political embarrassment, and a variety of others. Costs may be borne by the individuals who are affected, the corporations they work for, or they may involve macroeconomic costs to society.

Cost-Benefit analysis: Part of the management decision-making process in which the costs and benefits of each countermeasure alternative are compared and the most appropriate alternative is selected. Costs include the cost of the tangible materials, and also the on-going operational costs associated with the countermeasure implementation.

Countermeasures: An action taken or a physical capability provided whose principal purpose is to reduce or eliminate one or more vulnerabilities. The countermeasure may also affect the threat(s) (intent and/or capability) as well as the asset's value. The cost of a countermeasure may be monetary, but may also include non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

Countermeasures analysis: A comparison of the expected effectiveness of the existing countermeasures for a given threat against the level of effectiveness judged to be required in order to determine the need for enhanced security measures.

Cyber security: Protection of critical information systems including hardware, software, infrastructure, and data from loss, corruption, theft, or damage.

Delay: A countermeasures strategy that is intended to provide various barriers to slow the progress of an adversary in penetrating a site to prevent an attack or theft, or in leaving a restricted area to assist in apprehension and prevention of theft.

Detection: A countermeasures strategy to that is intended to identify an adversary attempting to commit a security event or other criminal activity in order to provide real-time observation as well as post-incident analysis of the activities and identity of the adversary.

Deterrence: A countermeasures strategy that is intended to prevent or discourage the occurrence of a breach of security by means of fear or doubt. Physical security systems such as warning signs, lights, uniformed guards, cameras, bars are examples of countermeasures that provide deterrence.

Hazard: A situation with the potential for harm.

Intelligence: Information to characterize specific or general threats including the motivation, capabilities, and activities of adversaries.

Intent: A course of action that an adversary intends to follow.

Layers of protection: A concept whereby several independent devices, systems, or actions are provided to reduce the likelihood and severity of an undesirable event.

Likelihood of adversary success: The potential for causing a catastrophic event by defeating the countermeasures. LAS is an estimate that the security countermeasures will thwart or withstand the attempted attack, or if the attack will circumvent or exceed the existing security measures. This measure represents a surrogate for the conditional probability of success of the event.

Mitigation: The act of causing a consequence to be less severe.

Physical security: Security systems and architectural features that are intended to improve protection. Examples include fencing, doors, gates, walls, turnstiles, locks, motion detectors, vehicle barriers, and hardened glass.

Process Hazard Analysis (PHA): A hazard evaluation of broad scope that identifies and analyzes the significance of hazardous situations associated with a process or activity.

Response: The act of reacting to detected or actual criminal activity either immediately following detection or post-incident.

Risk: The potential for damage to or loss of an asset. Risk, in the context of process security, is the potential for a catastrophic outcome to be realized. Examples of the catastrophic outcomes that are typically of interest include an intentional release of hazardous materials to the atmosphere, or the theft of hazardous materials that could later be used as weapons, or the contamination of hazardous materials that may later harm the public, or the economic costs of the damage or disruption of a process.

Risk assessment: Risk (R) assessment is the process of determining the likelihood of an adversary (T) successfully exploiting vulnerability (V) and the resulting degree of consequences (C) on an asset. A risk assessment provides the basis for rank ordering of risks and thus establishing priorities for the application of countermeasures.

Safeguard: Any device, system or action that either would likely interrupt the chain of events following an initiating event or that would mitigate the consequences.⁴

Security layers of protection: Also known as concentric ‘rings of protection’, a concept of providing multiple independent and overlapping layers of protection in depth. For security purposes, this may include various layers of protection such as counter-surveillance, counterintelligence, physical security, and cyber security.

Security management system checklist: A checklist of desired features used by a facility to protect its assets.

Security plan: A document that describes an owner/operator’s plan to address security issues and related events, including security assessment and mitigation options. This includes security alert levels and response measures to security threats.

Security Vulnerability Assessment (SVA): A SVA is the process of determining the likelihood of an adversary successfully exploiting vulnerability, and the resulting degree of damage or impact. SVAs are not a quantitative risk analysis, but are performed qualitatively using the best judgment of security and safety professionals. The determination

of risk (qualitatively) is the desired outcome of the SVA, so that it provides the basis for rank ordering of the security-related risks and thus establishing priorities for the application of countermeasures.

Target attractiveness: An estimate of the value of a target to an adversary based on the factors shown below. Experience has shown that, particularly for terrorist attacks, certain targets better accomplish the objectives of the adversaries than do others. Since the SVA is a risk-based analytical approach, consideration must be given to these factors in defining the threat and in determining the need for any enhanced countermeasures.

- Potential for mass casualties/fatalities
- Extensive property damage
- Proximity to national assets or landmarks
- Possible disruption or damage to critical infrastructure
- Disruption of the national, regional or local economy
- Ease of access to target
- Media attention or possible interest of the media
- Company reputation and brand exposure

Technical security: Electronic systems for increased protection or for other security purposes including access control systems, card readers, keypads, electric locks, remote control openers, alarm systems, intrusion detection equipment, annunciating and reporting systems, central stations monitoring, video surveillance equipment, voice communications systems, listening devices, computer security, encryption, data auditing, and scanners.

Terrorism: The FBI defines terrorism as, “the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”

Threat: Any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Threat categories: Adversaries may be categorized as occurring from three general areas:

- Insiders
- Outsiders
- Insiders working in collusion with outsiders

Undesirable events: An event that results in a loss of an asset, whether it is a loss of capability, life, property, or equipment.

Vulnerabilities: Any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings, or operational and personnel practices.

Abbreviations and Acronyms

A	Attractiveness
ACC	American Chemistry Council
AT	Target attractiveness
AIChE	American Institute of Chemical Engineers
API	American Petroleum Institute
AWCS	Accidental Worst-Case Scenario
C	Consequence
CCPS	Center for Chemical Process Safety of the American Institute of Chemical Engineers (AIChE)
CCTV	Closed Circuit Television
CEPPO	Chemical Emergency Preparedness and Prevention Office (USEPA)
CMP	Crisis Management Plan
CSMS	Chemical Security Management System
CW	Chemical Weapons
CWC	Chemical Weapons Convention
D	Difficulty of Attack
DCS	Distributed Control Systems
DHS	Department of Homeland Security
DOE	Department of Energy
DOT	U. S. Department of Transportation
EHS	Environmental, Health, and Safety
EPA	U. S. Environmental Protection Agency
ERP	Emergency Response Process
EHS	Environmental, Health, and Safety
FBI	U. S. Federal Bureau of Investigation
FC	Facility Characterization
HI	Hazard Identification
HSAS	Homeland Security Advisory System
IPL	Independent Protection Layer
IT	Information Technology
LA	Likelihood of Adversary Attack
LAS	Likelihood of Adversary Success
LOPA	Layer of Protection Analysis
MARSEC	Maritime Security Levels
MOC	Management of Change
NPRA	National Petrochemical and Refiners Association
OSHA	Occupational Safety and Health Administration
PHA	Process Hazard Analysis
PLC	Programmable Logic Controller
PSI	Process Safety Information
PSM	Process Safety Management (Also refers to requirements of 29 <i>CFR</i> 1910.119)
R	Risk
RMP	Risk Management Process (Also refers to requirements of EPA 40 <i>CFR</i> Part 68)
S	Severity of the Consequences
SOCMA	Synthetic Organic Chemical Manufacturers Association
SOP	Standard Operating Procedure
SVA	Security Vulnerability Assessment
T	Threat
TSA	Transportation Security Agency
V	Vulnerability
WMD	Weapons of Mass Destruction

