Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

ANSI/API STANDARD 780
FIRST EDITION, MAY 2013

AMERICAN PETROLEUM INSTITUTE

Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

Users of this Standard should not rely exclusively on the information contained in this document. Sound business, scientific, engineering, and safety judgment should be used in employing the information contained herein.

Work sites and equipment operations may differ. Users are solely responsible for assessing their specific equipment and premises in determining the appropriateness of applying the Standard. At all times users should employ sound business, scientific, engineering, and judgment safety when using this Standard.

Foreword

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Shall: As used in a standard, "shall" denotes a minimum requirement in order to conform to the specification.

Should: As used in a standard, "should" denotes a recommendation or that which is advised but not required in order to conform to the specification.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 1220 L Street, NW, Washington, DC 20005. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 1220 L Street, NW, Washington, DC 20005.

Suggested revisions are invited and should be submitted to the Standards Department, API, 1220 L Street, NW, Washington, DC 20005, standards@api.org.

Contents

Contents

Figures

Contents

Page

Tables

Introduction

API developed this security risk assessment (SRA) methodology as a universal approach for assessing security risk at petroleum and petrochemical facilities. The information contained herein has been developed in cooperation with government and industry and is intended to help oil and gas companies, petroleum refiners, pipeline operators, petrochemical manufacturers, and other segments of the petroleum industry or other similar industries maintain and strengthen their corporate security through a structured and standardized SRA methodology. This document contains a standard methodology and guidance for use including examples.

This standard describes a methodology that can be applied to a broad range of assets and operations beyond the typical operating facilities of the industry. This includes other assets containing hazardous materials such as chemical, refining and petrochemical manufacturing operations, pipelines, and transportation operations including truck, marine, and rail. It also can be used at a wide variety of nonhydrocarbon types of assets and is applicable as a general purpose SRA methodology. The methodology is suitable for assisting with compliance to regulations, such as the U.S. Department of Homeland Security's *Chemical Facility Anti-terrorism Standards,* 6 *CFR* Part 27.

The focus of this standard was to expand the successful first and second editions but not to change the basic methodology. Overall, the methodology is well received and appreciated by a wide variety of security professionals in the petroleum and petrochemical industry as well as by others who want to use a generalized all risk security vulnerability assessment methodology in the private and public sectors. The major changes include renaming the methodology from a security vulnerability analysis methodology to a SRA methodology in order to reflect the full scope of the analysis as a risk assessment vs a vulnerability analysis, which is only one step of the methodology. The update considered improvements based on recent developments and experiences from practical use. Also, additional details were included to further assist users in efficiently using the approach in a standardized manner particularly in the ranking of likelihood. The terminology was changed from vulnerability assessment to risk assessment since the five-step process is a risk assessment including characterization, threat assessment, vulnerability assessment, risk evaluation, and risk treatment steps.

The popularity of the methodology is increasing worldwide, and many companies have now adopted it as a corporate standard. However, there are several other risk assessment techniques and methods available to industry, many 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.

Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

1 Scope

1.1 General

This Standard was prepared by a security risk assessment (SRA) committee of API to assist the petroleum and petrochemical industries in understanding conducting SRAs. The standard describes the recommended approach for assessing security risk widely applicable to the types of facilities operated by the industry and the security issues the industry faces. The standard is intended for those responsible for conducting SRAs and managing security at these facilities. The method described in this standard is widely applicable to a full spectrum of security issues from theft to insider sabotage to terrorism.

The API SRA methodology was developed for the petroleum and petrochemical industry, for a broad variety of both fixed and mobile applications. This Standard describes a single methodology rather than a general framework for SRAs, but the methodology is flexible and adaptable to the needs of the user. This methodology constitutes one approach for assessing security vulnerabilities at petroleum and petrochemical industry facilities. However, there are other risk assessment techniques and methods available to industry, all of which share common risk assessment elements.

Ultimately, it is the responsibility of the user to choose the SRA methodology and depth of analysis that best meet the needs of the specific operation. Differences in geographic location, type of operations, experience and preferences of assessors, and on-site quantities of hazardous substances are but a few of the many factors to consider in determining the level of SRA that is required to undertake. This standard should also be considered in light of applicable laws and regulations.

1.2 Overview

Users should manage security risks by first identifying and analyzing the threats, consequences, and vulnerabilities facing a facility or operation by conducting a formal SRA. A SRA is a systematic process that evaluates the likelihood that a given threat factor (e.g. activist, criminal, disgruntled insider, terrorist) will be successful in committing an intentional act (e.g. damage, theft) against an asset resulting in a negative consequence (e.g. loss of life, economic loss, or loss of continuity of operations). It can consider the potential severity of consequences and impacts to the facility or company itself, to the surrounding community, and on the supply chain.

The objective of conducting a SRA is to assess security risks as a means to assist management in understanding the risks facing the organization and in making better informed decisions on the adequacy of or need for additional countermeasures to address the threats, vulnerabilities, and potential consequences.

The API SRA methodology is a team-based, standardized approach that combines the multiple skills and knowledge of the various participants to provide a more complete SRA of the facility or operation. Depending on the type and size of the facility or scope of the study, the SRA team may include individuals with knowledge of physical and cyber security, facility and process design and operations, safety, logistics, emergency response, management, and other disciplines as necessary.

1.3 Sequential Activities

The API SRA methodology includes the following five sequential steps.

1) *Characterization*—Characterize the facility or operation to understand what critical assets need to be secured, their importance, and their infrastructure dependencies and interdependencies;

2) *Threat Assessment*—Identify and characterize threats against those assets and evaluate the assets in terms of attractiveness of the targets to each threat and the consequences if they are damaged, compromised, or stolen.

3) *Vulnerability Assessment*—Identify potential security vulnerabilities that enhance the probability that the threat will successfully accomplish the act.

4) *Risk Evaluation*—Determine the risk represented by these events or conditions by determining the likelihood of a successful event and the maximum credible consequences of an event if it were to occur; rank the risk of the event occurring and, if it is determined to exceed risk guidelines, make recommendations for lowering the risk.

5) *Risk Treatment*—Identify and evaluate risk mitigation options (both net risk reduction and benefit/cost analyses) and reassess risk to ensure adequate countermeasures are being applied. Evaluate the appropriate response capabilities for security events and the ability of the operation or facility to adjust its operations to meet its goals in recovering from the incident.

2 Normative References

This document contains no normative references. A list of documents and articles associated with API 780 and SRA are included in the bibliography.

3 Terms, Definitions, Acronyms, Abbreviations, and Symbols

3.1 Terms and Definitions

For the purposes of this document, the following definitions apply.

3.1.1
act
The assumed malevolent scenario under study.

3.1.2
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 a threat, as well as an owner, although the nature and magnitude of those values may differ.

3.1.3
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.

3.1.4
attack method
Manner and means, including the weapon and delivery method, a threat may use to cause harm on a target.

3.1.5
attack path
Steps that a threat takes or may take to plan, prepare for, and execute an attack.

3.1.6
attractiveness
A
An estimate of the value of a target to a threat. Consideration shall be given to the following 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.

3.1.7
baseline risk
Current level of risk that takes into account existing risk mitigation measures.

3.1.8
benefit
Amount of expected risk reduction based on the overall effectiveness of countermeasures.

3.1.9
capability
Means to accomplish a mission, function, or objective.

3.1.10
consequence
C
The outcome of an event, commonly measured in four ways—human, economic, mission, and psychological—but may also include other factors such as impact on the environment.

3.1.11
consequence assessment
Product or process of identifying or evaluating the potential or actual effects of an event, incident, or occurrence.

3.1.12
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.

3.1.13
cost-benefit analysis
The decision-making process in which the costs and benefits of each countermeasure alternative are compared and the most appropriate alternative is selected.

3.1.14
countermeasure
An action, measure, or device intended to reduce an identified risk.

3.1.15
countermeasures analysis
A comparison of the expected effectiveness of the existing countermeasures for a given risk against the level of effectiveness judged to be required in order to determine the need for enhanced security measures.

3.1.16
criticality
Importance to a mission, function, or continuity of operations.

3.1.17
criticality assessment
Product or process of systematically identifying, evaluating, and prioritizing based on the importance of an impact to mission(s), function(s), or continuity of operations.

3.1.18
cyber security
Protection of critical information systems including hardware, software, infrastructure, and data from loss, corruption, theft, or damage.

3.1.19
delay
A countermeasures strategy that is intended to provide various barriers to slow the progress of a threat in penetrating a site to prevent an attack or theft or in leaving a restricted area to assist in apprehension and prevention of theft.

3.1.20
detect/detection
A countermeasures strategy that is intended to identify a threat 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 threat.

3.1.21
deter/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, and bars are examples of countermeasures that provide deterrence.

3.1.22
direct consequence
Effect that is an immediate result of an event, incident, or occurrence.

3.1.23
frequency
Number of occurrences of an event per defined period of time or number of trials.

3.1.24
hazard
Natural or man-made source or cause of harm or difficulty.

3.1.25
incident
Occurrence, caused by either human action or natural phenomena, which may cause harm and may require action.

3.1.26
intelligence
Information to characterize specific or general threats when considering a threat's motivation, capabilities, and activities.

3.1.27
intent
A course of action that a threat intends to follow.

3.1.28
layers of protection
A concept whereby several independent devices, systems, or actions are provided to reduce the likelihood and severity of an undesirable event.

3.1.29
likelihood
L
Chance of something happening, whether defined, measured, or estimated objectively or subjectively or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities. Likelihood of the act is a function of two subcomponents, L_1 and L_2.

3.1.30
likelihood of success of the act
L_2
The potential for causing the event by defeating the countermeasures. L_2 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. (Conditional probability of success of the event is the measure of vulnerability (V), so therefore L_2 and V are synonymous: $L_2 = V$.)

3.1.31
likelihood of the act
L_1
The potential for a threat to target and to attempt to execute a security act against an asset. This is a function of the threat and the attractiveness of the asset to the threat.

3.1.32
mitigation
Ongoing and sustained action to reduce the probability of, or lessen the impact of, an adverse incident.

3.1.33
physical security
Security systems and architectural features that are intended to improve protection.

3.1.34
probability
Numerical value between zero and one assigned to a random event (which is a subset of the sample space) in such a way that the assigned number obeys three axioms:

1) the probability of the random event “A” must be equal to, or lie between, zero and one;

2) the probability that the outcome is within the sample space must equal one; and

3) the probability that the random event “A” or “B” occurs must equal the probability of the random event “A” plus the probability of the random event “B” for any two mutually exclusive events .

3.1.35
process hazard analysis
A safety hazard evaluation of broad scope that identifies and analyzes the significance of hazardous situations associated with a process or activity.

3.1.36
recovery
The ability of a site to withstand and execute service and site restoration plans for affected assets and the reconstitution of operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents.

3.1.37
relative risk
Measure of risk that represents the ratio of risks when compared to each other or a control.

3.1.38
residual risk
Risk that remains after risk management measures have been implemented.

3.1.39
resilience/resiliency
The ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions. In the context of energy security, resilience is measured in terms of robustness, resourcefulness, and rapid recovery.

3.1.40
respond/response
The act of reacting to detected or actual criminal activity either immediately following detection or post-incident.

3.1.41
risk
R
The potential for damage to or loss of an asset. Risk, in the context of security, is the potential for a negative outcome to be realized from an intentional act. For chemical and petroleum facilities, examples of the catastrophic outcomes that are typically of interest include an intentional release of hazardous materials to the atmosphere, the theft of hazardous materials that could later be used as improvised weapons, the contamination of hazardous materials that may later harm the public, or the economic costs of the damage or disruption of a process. For the API SRA methodology, risk can be expressed as:

— existing risk—the estimate of risk with existing countermeasures (R_1)—and

— proposed risk—the estimate of risk with the addition of proposed countermeasures (R_2).

3.1.42
risk acceptance
Explicit or implicit decision not to take an action that would affect all or part of a particular risk.

3.1.43
risk analysis
Systematic examination of the components and characteristics of risk.

3.1.44
risk assessment
Risk (R) assessment is the process of determining the likelihood of a threat (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.

3.1.45
risk assessment methodology
Set of methods, principles, or rules used to identify and assess risks and to form priorities, develop courses of action, and inform decision making.

3.1.46
risk management
Process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

3.1.47
risk matrix
Tool for ranking and displaying components of risk in an array. Risk matrices are user defined.

3.1.48
risk mitigation
Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences.

3.1.49
risk tolerance
Degree to which an entity, asset, system, network, or geographic area is willing to accept risk.

3.1.50
risk transfer
Action taken to manage risk that shifts some or all of the risk to another entity, asset, system, network, or geographic area.

3.1.51
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.

3.1.52
scenario
Hypothetical situation comprised of an intentional act, an assumed threat, a set of consequences, and associated countermeasures to address the scenario.

3.1.53
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 countersurveillance, counterintelligence, physical security, and cyber security. A second consideration is the balance of the security measures such that equivalent risk exists regardless of the threat's pathway or method.

3.1.54
security plan
A document that describes an owner's/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.

3.1.55
security risk
R_S
The likelihood of a threat successfully exploiting vulnerability and the resulting degree of damage or impact.

3.1.56
security risk assessment
SRA
A SRA is a risk assessment for the purposes of determining security risk.

3.1.57
system
Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.

3.1.58
target
Asset, network, system, or geographic area chosen by a threat to be impacted by an attack.

3.1.59
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.

3.1.60
terrorism
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.

3.1.61
threat
T
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 capability and intent of a threat to undertake actions that would be detrimental to critical assets. Threat encompasses any individual, group, organization, or government that conducts activities or has the intention and capability to conduct activities detrimental to critical assets. A threat could include intelligence services of host nations, or third-party nations, political and terrorist groups, criminals, rogue employees, cyber criminals, and private interests.

3.1.62
threat assessment
Product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that has or indicates the potential to harm life, information, operations, and/or property.

3.1.63
threat categories
Adversaries may be categorized as occurring from three general areas:

— internal threats,

— external threat,

— internal threats working in collusion with external threats.

3.1.64
unacceptable risk
Level of risk at which, given costs and benefits associated with further risk reduction measures, action is deemed to be warranted at a given point in time.

3.1.65
uncertainty
Degree to which a calculated, estimated, or observed value may deviate from the true value.

3.1.66
undesirable events
An event that results in a loss of an asset, whether it is a loss of capability, life, property, or equipment.

3.1.67
vulnerability
V
A weakness that can be exploited by a threat to gain access to an asset, to include building characteristics, equipment properties, personnel behavior, locations of personnel, equipment, or operational and personnel practices.

3.1.68
vulnerability assessment
Product or process of identifying physical features or operational attributes that renders an entity, asset, system, network, or geographic area susceptible or exposed to hazards.

3.2 Acronyms, Abbreviations, and Symbols

For the purposes of this document, the following acronyms, abbreviations, and symbols apply.

A	attractiveness
C	consequence (initial consequence without consideration of any existing countermeasures)
C_1	severity of scenario-specific consequences

C_2	severity of scenario-specific consequences, presuming the implementation of all countermeasures recommended by the SRA team
CCTV	closed circuit television
CFR	*Code of Federal Regulations*
DHS	U.S. Department of Homeland Security
EPA	U.S. Environmental Protection Agency
IT	information technology
L_1	likelihood of unmitigated adversary attack ($T \times A$)
L_2	$L_2 = V$, likelihood of attack success based on vulnerability and existing countermeasures
OSHA	U.S. Occupational Safety and Health Administration
R	risk
R_s	security risk
R_1	conditional risk, function of L_1 ($A \times T$) $\times L_2$ (where $L_2 = V$) and scenario consequence C_1 on the risk matrix
R_2	residual risk, function of L_3, V_2, and C_2 including recommendations on the risk matrix
SCADA	supervisory control and data acquisition system
SOC	Security operations center
SRA	security risk assessment
T	threat
TR	target rating
V	$V = L_2$, likelihood of success of the act based on vulnerability and existing countermeasures
V_2	likelihood of success of the act subsequent to recommended upgrades/countermeasures
VBIED	vehicle borne improvised explosive device

4 Introduction to SRA Concepts

4.1 General

A SRA is the process that includes determining the risk of security events and then, based on this assessment, making judgments on the adequacy of existing countermeasures and the need for and value of implementing additional countermeasures. To understand how to conduct a SRA, key terms and concepts are explained in this section.

4.2 Security Risk Assessment and Security Management Principles

The premise of this Standard is that security risks should be managed in a risk-based, performance-oriented management process to ensure the security of assets and the protection of the public, the environment, workers, and the continuity of the business. A SRA is a management tool that should be used to assist in accomplishing this task and to help the owner/operator in making decisions on the need for and value of security enhancements. Factors used in the SRA methodology include the threat, the attractiveness of the asset to adversaries, the possible consequences and impacts of an incident, and the degree of vulnerability. For example, in the case of terrorist threats, higher risk sites may be those that have critical importance, are attractive targets to the threat, have a high level of consequences, and where the level of vulnerability and threat is high.

SRAs can be quantitative or qualitative in nature. The SRA can be performed semiquantitatively by using a risk matrix and assessed by using the best judgment of the SRA team. This may include bounding the risk in expected ranges of frequency and consequences as defined by the user. The expected outcome is a semiquantitative 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.

The API SRA methodology does not prescribe a single risk acceptance criteria or formula to define risk using these variables as the use may adapt company-specific variables in line with the risk assessment framework to make these decisions. Ultimately each company should develop its own risk assessment guidance including a risk decision-making framework and criteria for tolerability of risks. This standard includes a risk ranking process that will assist in framing risks across the enterprise if standardized. However, it is recognized that the uncertainties associated with estimating certain low probability, high consequence events, such as the threat of terrorism, make the process imprecise.

The user defines a certain number of credible scenarios to produce a representative risk estimate. Then the user shall consider the following five basic strategies when conducting the analysis and assessing adequacy of countermeasures.

1) *Deter*—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 elements such as warning signs, lights, uniformed guards, cameras, and fences are examples of visible countermeasures that provide deterrence in addition to their primary security purpose.

2) *Detect*—A countermeasures strategy that is intended to identify a threat attempting to commit a security event in order to provide real-time observation as well as post-incident analysis of the activities and identity of the threat. Examples are patrols, alarm systems, and closed circuit television (CCTV) cameras.

3) *Delay*—A countermeasures strategy that is intended to provide various barriers to slow the progress of a threat in penetrating a site to prevent an attack or theft, or in leaving a restricted area to assist in interdiction. Examples include access control checkpoints, door locks, and bars on windows.

4) *Respond*—The act of reacting to detected malevolent activity. This may include activities to interdict, prevent damage or further loss, or control the incident. Protective forces, response plans, and emergency shutdown systems are typical examples.

5) *Recover*—Means such as redundancy or resiliency to mitigate the effects of the security event and to continue or return operations expeditiously with minimum collateral damages, downtime, and other impacts. Backup servers, spare long-lead equipment, or extra capacity are examples of recovery capability.

Appropriate strategies for managing security may vary widely depending on the individual circumstances of the operation, including the type of operation and the attendant threats. This standard does not prescribe specific security measures but rather provides the means to identify, analyze, and reduce vulnerabilities. The specific situations should be evaluated individually by local management using best judgment of applicable practices. Appropriate security risk management decisions should be made commensurate with the risks. This flexible approach recognizes that there is not a prescribed approach to security in the petroleum and petrochemical industry and that resources are best applied on a risk basis.

Asset owners or operators should seek out assistance and coordinate efforts with appropriate law enforcement, government authorities, local emergency services, and local emergency planning committees for integrated planning and response. Owners/operators should obtain and share intelligence, coordinate training, and allocate necessary resources to help deter attacks and to manage security events commensurate with the identified threats.

4.3 Risk Definition for SRA and Key Variables

For the purposes of the API SRA, the definition of security risk is shown in Figure 1. Key variables are explained in the following subsections. *The risk that is being analyzed for the SRA is defined as an expression of the likelihood* (L) *that a defined threat* (T) *will find an asset attractive* (A) *and successfully commit an act against it, taking advantage of vulnerability* (V) *to cause a given set of security consequences* (C). The SRA process may be used to evaluate one or more specific scenarios or to sum the risk of the entire set of security scenarios of issue into an operational or facility-wide risk estimate.

API SRA Methodology

Security risk (R_S) is a function of consequences, vulnerability, and threat

or

R_S = a function of (C, V, T)

where

C is the direct and indirect consequence of a successful act against an asset;

V is the vulnerability of the asset to the act;

T is the threat associated with the act;

R_S is the the likelihood of a successful act against an asset assuming both the likelihood of the act occurring (L_1) and the likelihood of success (L_2) causing a given set of consequences.

Therefore, R_S = a function of (C, L_1, L_2) or $R_S = C$, ($A \times T$), V.

Figure 1—Security Risk Definition

For the SRA, the risk of the security event shall be estimated semiquantitatively by using a risk matrix unless a quantitative analysis is to be done. The risk matrix is a tool for decision-making and the exact matrix used is determined by the user so that it is most applicable to the situation. The API SRA methodology does not prescribe the risk matrix that must be used to comply with this standard. However, if the user does not adopt the suggested matrix, a similar matrix shall be developed. The user should consider adopting the same matrix and applying it consistently throughout the enterprise for uniform decision-making.

The decision on ranking of severity of consequence and likelihood factors shall be based on the consensus judgment of a team of knowledgeable persons and subject matter experts. They estimate how the likelihood and consequences of an undesired event scenario relatively compares to other scenarios and/or on an absolute scale based on best available information, using experience and expertise of the team to make sound risk management decisions. Using a risk matrix as a decision aide, the analysts define the degree of risk based on several factors and use this information to compare to other risks or to incorporate risk tolerance criteria.

The API SRA methodology employs a risk-based screening process in the first step of the process to focus the analysis and resource attention on higher risk, more critical events. The key variables considered in the risk screening analysis are consequences and attractiveness. If either of these variables falls below the threshold of risk tolerance acceptable to the user, the asset may be screened out from further specific consideration. Later, the complete set of risk variables is used to evaluate the risk and to determine the need for additional specific countermeasures.

4.4 Likelihood (L)

Likelihood (L) is an estimate of the probability or frequency that a given act will result in a given consequence. It is both a function of the threat seeking out the asset and attempting the act as well as the successful execution of the act to achieve the threat's goals. Likelihood is a function of several factors including the degree of threat (T), as determined by analyzing the threat's history, capabilities, motivation, and intent, while incorporating relevant information such as loss statistics, law enforcement data, and professional judgment.

Likelihood is a function of the chance of being targeted for an act and the conditional chance of a successful attack (i.e. both planning and execution) given the threat (which considers the threat's actions and choices) and given the options available against existing security measures. The combination of the two factors threat (T) and attractiveness (A) produce a surrogate estimate for the likelihood of the act (L_1) for each scenario, which is either a probability of the event or a frequency over a given period of time such as the life of the operation. Vulnerability (V) is a surrogate for the likelihood of expected success (L_2) for each scenario ($L_2 = V$).

A more detailed analysis of the factors involved in estimating the likelihood of the event is necessary in order to present risk against a two-dimensional risk matrix of likelihood (L) versus consequences (C) and results in two components of likelihood, L_1 and L_2.

— *Likelihood of the Act (L_1)*—The potential for a threat to target and to attempt to execute a security event against an asset. This is a function of the threat and the attractiveness of the asset to the threat. The threat is assumed to target assets to which it is attracted, so the measure of L_1 is the product of $T \times A$, where A is the attractiveness of the asset to the threat; therefore, L_1 is the likelihood of an attempted act against an asset. L_1 represents a surrogate for the likelihood of the act.

$$L_1 = A \times T$$

— *Likelihood of Success of the Act (L_2)*—The potential for causing the consequences estimated by performing the act and defeating the countermeasures. L_2 is an estimate of the likelihood that the security countermeasures will thwart or withstand the attempted attack or, conversely, the likelihood that the attack will circumvent or exceed the existing security measures. L_2 represents a surrogate for the conditional probability of success of the event, or in other words, the vulnerability (V) of the asset, which can be expressed as a numeric value ranging from 1 to 5 that corresponds to a conditional probability that the threat will succeed if the event occurs.

$$L_2 = V$$

4.5 Consequences (C)

The severity of the consequences of a security event at a facility or operation and the resulting impacts of the event should be expressed in terms of the degree of injury, damage, business interruption costs, or damage to good will toward the organization (reputational damage) that would result if there were a successful act. Acts may involve effects that are more severe or have different outcomes than those expected with accidental risk or natural events since they are intentional and targeted but may have some similarities. All relevant and significant consequences from the following list shall be included as a minimum in the SRA performed to this Standard:

— casualties,

— environment,

— replacement cost,

— business interruption,

— damage to reputation/negative publicity.

Consequence shall be further evaluated specifically for each scenario of significance that passed the screening step. For any scenario where the team determined a need for a reduction in risk, the expected risk from the addition of the recommended countermeasures shall be evaluated by making a secondary estimate of consequences.

— C_1—Mitigated consequence is the severity of consequence of the specific scenario, considering existing countermeasures, to establish a baseline of existing credible loss.

— C_2—Severity of consequence of the specific scenario given the expected aggregate reduction based on new countermeasures.

The estimate of consequences may be different in magnitude or scope for terrorism events than the estimate normally anticipated for other forms of security events. In the case of terrorism events, adversaries could presumably want to cause maximize credible damage, so a worst credible security consequence level estimate should be defined, but the team needs to define the credible estimate of consequences specific to each scenario.

Critical infrastructure will likely have dependencies and interdependencies that should be considered in determining the magnitude of the consequences. Consequences shall be considered 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 may be used to screen low value assets from further consideration (i.e. if the consequences related to a certain asset fall at or below the level acceptable to the owner/operator, then the SRA team may decide not to pursue further risk analysis for that particular asset).

4.6 Threat (T)

Threat is 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 a threat to undertake actions that would be detrimental to valued assets. Sources of threats may be categorized as:

— criminals (e.g. white collar, cyber, organized, opportunists);

— activists (pressure groups, single-issue zealots);

— terrorists (international or domestic);

— disgruntled personnel.

Threat is a function of the known patterns of potential adversaries and the threat's existence, intent, motivation, and capabilities. Different adversaries may pose different threats to various assets and so threat can be generally and/or specifically estimated for each asset-scenario pairing. Threat is considered against a series of individual events or as an overall threat to an operation depending on the level of resolution possible or necessary. Threat can be expressed as a frequency of an act or a probability of an act over time. Threat can be expressed as an integer value ranging from 1 through 5 based on the degree to which a threat has the capability and intent to harm a specific asset by way of the scenario under analysis. This rating can be evaluated as a function of such factors as:

— credible existence of a threat for the location of the asset;

— intelligence about the threat, including general history of events;

— suspected intent or motivation;

— intelligence about the threat specific to the company or facility being analyzed;

— assessed capability and ability to execute the act.

Threats may have a violent intent, such as workplace violence from disgruntled personnel, or nonviolent intent, such as an unarmed thief attempting to steal property or demonstrators protesting against an organization. The consequence of their actions can be immediate (such as terrorists causing a chemical release) or delayed (such as terrorist stealing chemicals for the purpose of part of a more complex or strategic plan of attack).

Threat information shall be considered by the user to understand those adversaries interested in the assets of the facility, their operating history, their methods and capabilities, their possible plans, and what motivates them. This information shall then be used to develop an assumed threat or set of threats that form the basis of the risk assessment.

Threats from the following three categories shall be included in the SRA:

— internal,

— external,

— collusion (internal and external).

Depending on the scope of the analysis, each applicable threat type shall be evaluated against each critical asset (this is referred to as the threat-asset pairing) to determine the attractiveness (A) of that asset from the threat's perspective. The threat (T) factor multiplied by the attractiveness factor becomes an initial indicator of the degree of likelihood of the act (L_1) or $L_1 = A \times T$.

4.7 Attractiveness (A)

Attractiveness is a factor that modifies the threat estimate to result in the likelihood of the security event for a specific act or against a specific asset. This factor can be evaluated as a composite estimate based on such factors as:

— the perceived value of a target to the threat,

— the threat's choice of targets to avoid discovery and to maximize the probability of success.

The variable A can be assigned an integer value from 1 through 5 based on the attractiveness factor assessment ("1" being very low/very unattractive and "5" being very high/very attractive). This may be related to a conditional probability between 0.0 and 1.0 in increments of 0.2 for each of the five levels as an additional means of relating to the attractiveness estimate. This suggested scheme gives the team a framework for risk decision-making either on a relative or absolute scale. Then attractiveness can be used as a factor to lower the expectation that the threat would attack the particular asset if the attractiveness is considered.

Not all assets should be considered as being of equal value or interest to all threats. A basic assumption of the SRA process is that this perception of value from a threat's perspective can serve as a targeting factor that influences the likelihood of a security event. Asset attractiveness shall be used to provide an estimate of the real or perceived value of a target to a threat. The analysts should base the assumption of attractiveness on relevant attractiveness factors such as those shown in Figure 2.

Depending on the type of threat and its potential targets, the threat is assumed to run through a decision analysis depending on threat factors (the threat's intent, capabilities, and motivation), site and asset vulnerability factors, potential consequences, and impact factors that lead the threat to the decision to attempt an act and to choose a modus operandi that includes selecting pathways, timing, and the mode of the act.

During the SRA, the attractiveness of each critical asset is considered and evaluated based on the threat's intentions or anticipated level of interest in the target. Potential threat strategies shall be developed around the potential targets for each credible and related potential threat. This factor, along with that of consequences, shall be used to screen facilities from more specific scenario analysis and from further specific countermeasures considerations.

4.8 Vulnerability (V)

Vulnerability shall be considered in the analysis and is defined as any weakness that can be exploited by a threat in order to gain access to an asset and to succeed in a malevolent act against that asset. Vulnerability is determined by evaluating the inability to Deter, Detect, Delay, Respond to, and Recover from a threat in a manner sufficient to limit the likelihood of success of the threat, or to reduce the impacts of the event through such measures as interdiction, response, suppression of effects, emergency management, and resilience.

Vulnerability (V) is expressed as a numeric value of 1 through 5 reflecting a conditional probability as an integer value between 1 and 5 (1 being very low/very unlikely to succeed and 5 being very high/very likely to succeed). This factor may be related to attractiveness (A) in that it is possible that a less vulnerable (and therefore less attractive) site may reduce the likelihood of the asset being targeted by the threat. Vulnerability is expressed as a surrogate for the likelihood of expected success (L_2) for each scenario; $L_2 = V$. Therefore, if a given threat attempts to cause an act against an asset, the V factor is considered to determine the likelihood of success.

Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical security, or operational security practices. Vulnerabilities are analyzed by considering multiple potential specific sequences of

API SRA Methodology
Type of effect desired: — maximizing the general amount of, or selectively targeting a particular asset for, theft or diversion for personal or organizational gain (physical or cyber theft); — causing harm to a particular person or organization either physically or indirectly (direct injury or damage, business interruption, economic loss to the facility and company); — potential for causing impact value based on adversary's objectives (media exposure, shock value, damage to company reputation); — potential for causing damage and economic loss to the geographic region (major disruptive event to regional resource or supplier); — potential for causing damage and economic loss to the corporate or national infrastructure (major disruptive event to supply chain).
Attributes of the target asset: — value of asset to the adversary (theft or damage for personal gain, noneconomic factors such as damaging the company reputation or brand, obtaining or damaging a prized iconic or symbolic target); — for chemical theft, usefulness of the chemical as a weapon or to cause collateral damage (whether it is a chemical or biological weapons precursor chemical or explosive, toxic, or flammable material that can be weaponized); — difficulty of act, including ease of access and degree of existing security measures (soft target vs hardened target); — recognition of the target while staging an act or while in the process of the act (ease of identifying the target).

Figure 2—Target Attractiveness Factors

events (a scenario-based approach). Any means of providing recovery from or resiliency to the impacts of the security event should be evaluated for consideration as mitigating factors to vulnerability. Factors related to resilience and the ability to recover from a given threat scenario shall be considered in order to adjust the vulnerability estimate, reflecting the value of redundancy and other mitigating elements that reduce the impact on replacement or business interruption.

5 SRA Approach

5.1 Concept and Relationship to Security Risk Management Process

The general philosophical approach of this Standard is threefold—first is to apply SRA assessment resources and, ultimately, to direct security resources where justified on a risk basis in accordance with the SRA results. The second attribute of the API SRA methodology is that it is adaptable and scalable to the needs of the analysts. Third, it is performance-based, allowing the analysts to determine the most appropriate security measures to manage the identified risks for the facility or operation.

Risk assessment is one element of a risk management process. The SRA process shall be revisited or reevaluated at a frequency determined by the owner/operator in order to maintain the currency of the SRA through monitoring and review, and there is continual opportunity to communicate and consult with stakeholders on all aspects of the process.

5.2 Conducting and Reviewing the SRA

The API SRA methodology can be applied at different stages of the overall security risk management lifecycle. The SRA should be performed for an initial assessment of risk, as well as for consideration of risk when significant changes to a facility or operation are planned or have been implemented. There are seven occasions when the SRA should be conducted or reviewed and then revised as necessary, as illustrated in Figure 3.

API SRA Methodology	
1)	An initial review of 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 as required depending on the degree of change, relevance of the existing study, and quality of the existing study).
3)	When a new process or operation is proposed and prior to implementation.
4)	When the threat substantially changes, at the discretion of the manager of the facility (revision or rework to reflect lessons learned and revised threat levels unless previously considered).
5)	After a significant security incident, at the discretion of the manager of the facility (revision or rework as determined to be necessary).
6)	Periodically to revalidate the SRA on a predetermined schedule (revision or rework as necessary).
7)	When any applicable regulatory requirement deadline causes a special requirement.

Figure 3—Recommended Times for Conducting and Reviewing the SRA

5.3 Validation and Prioritization of Risks

The user should 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 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) conducting a through a review of the SRA data and results. This review of the SRA method should be performed to ensure that the method has produced results that are validated by the reviewers. If the results are not consistent with the operator's understanding and expectation of system operation and risks, the operator should explore the reasons why, and make appropriate adjustments to the assumptions or data. Some additional criteria to evaluate the quality of a SRA include the following.

— Were 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 the conclusions and recommendations?

5.4 Risk-based Screening

The API SRA methodology is a comprehensive and systematic tool designed to thoroughly consider various risk factors in the assessment. It is also risk based to focus resources on the most important security issues. It begins with the SRA team gaining an understanding of the entire facility or operation, the associated assets, their critical functions, and the hazards and impacts if these assets or critical functions are compromised. This results in an understanding of which assets and functions are "critical" to the business operation.

Criticality of an asset or operation is defined in terms of the potential impact to the site employees, contractors, or visitors, community, the environment, and the company, as well as to the business continuity and economic importance of the asset or operation. For example, a storage tank of a toxic hazardous material may not be the most critical component of the operation of a process from an engineering or business perspective, but if attacked it has the greatest public impact so it may be given a higher priority for further analysis and special security countermeasures.

Critical assets are identified based on this screening of all assets related to the facility or operation. Next, the critical assets are reviewed in light of the threats. threats may have different objectives, so the critical asset list is reviewed from the perspective of each threat and an asset attractiveness ranking is determined. This factor is a quick measure of whether the threat would value damaging, compromising, or stealing the asset; this serves as both an indicator of the likelihood that a threat would want to attack this asset and as the record of the basis for that decision within the SRA.

Security issues exist at every facility or operation managed by the petroleum and petrochemical industry, but the threat of acts is not evenly distributed across the industry. This is captured by the factor of asset attractiveness, whereby certain assets are considered more likely to be of interest to adversaries than other assets. Target attractiveness is a targeting concept and is a dynamic consideration of the threat's preference. Based on many reported threat assessments, intelligence reports, and actual events available to the analysts, attractiveness factors shall be used to evaluate the attractiveness factors and to assign a ranking.

If an asset is both critical (based on value and consequences) and attractive, then the team shall consider it a "target asset" for that particular threat. A target asset shall receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities.

The API screening process contains the following factors:

1) attractiveness;

2) consequences (casualties, environmental, theft, operational continuity disruption, infrastructure damage and disruption, reputation, and economic).

Later in the SRA process, these two factors are also part of the analysis of specific scenarios and are used for evaluating an individual asset risk. However, the analysis is performed at this stage for screening the risk at a generalized facility or operational level, and later the analysis is performed at a target asset level where it is very specifically based on assumed causes. Note that attractiveness itself may be influenced by the factors of consequences and vulnerability. Attractiveness is an aggregate of factors, which encompasses the complexity of the targeting process.

Consequence and attractiveness are the dominant factors in determining risk at this stage of the process. In any target-rich environment where the potential number of targets poses a risk assessment 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 the need to conduct detailed assessments (as opposed to simpler checklist analyses or audits) and the order of priority for conducting those analyses.

Assets within the scope of the study shall receive a general security review. This is accomplished by the SRA team's consideration of each asset, which may also include a baseline security survey or other review in addition to the SRA. General security considerations may be found in security references that describe appropriate countermeasures for different security situations. Asset owners/operators should establish a comprehensive security strategy to protect against unauthorized access at the facility perimeter, and to control the access of all persons (whether authorized or not) while on the facility. Certain assets may need to be safeguarded with added layers of protection because of their attractiveness and the consequences of loss. The specific security countermeasures provided to those assets shall minimize risk by incorporating the concepts of deter, detect, delay, respond, and recover against credible threats.

For many studies there will be a lack of specific threat history for all of the risks that must be evaluated, particularly for high consequence events such as terrorism. As a result, when considering rare events the initial assumption should be made conservatively, but must be respectful of hazard potential and credible vulnerabilities, and adversaries' interest and capabilities. For example, it should be recognized that potential terrorist acts are generally credible at critical oil and gas facilities, but this concern is then tempered by the site-specific factors in order to screen out those assets or facilities where the specific threat under consideration may not be applicable.

In the absence of any data on threats, or where estimates of likelihood of attack are very low, users still may want to make an assumption of threat to set a challenge to the process and to determine the potential need to consider these threats in the security design. Certain threats may be determined as not credible and can be dismissed after documenting the reasons for dismissal.

6 SRA Approach

6.1 General

The API SRA standard is both a risk-based and performance-based methodology. The user must follow the general SRA method but may use customized methods to conduct the SRA so long as the process is consistent with the following five steps, the method considers all normative language in the standards, and the end result meets the same objective. The conceptual API SRA process is summarized in Figure 4 and is illustrated further in the flowcharts that follow in Figure 5 through Figure 7.

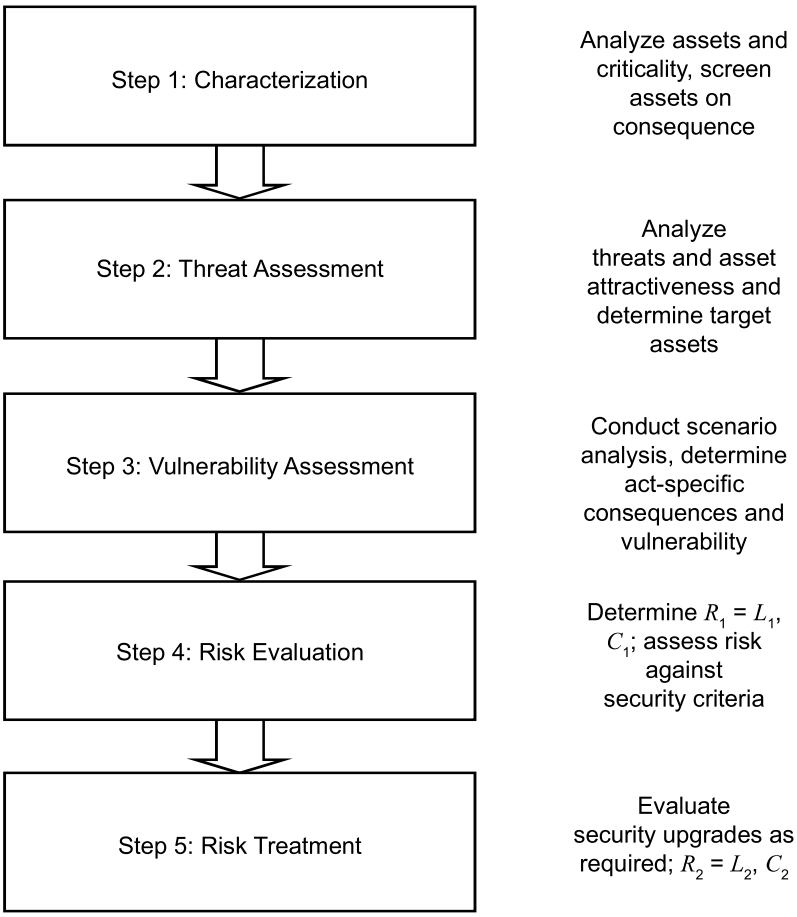

Figure 4—API Security Risk Assessment Methodology

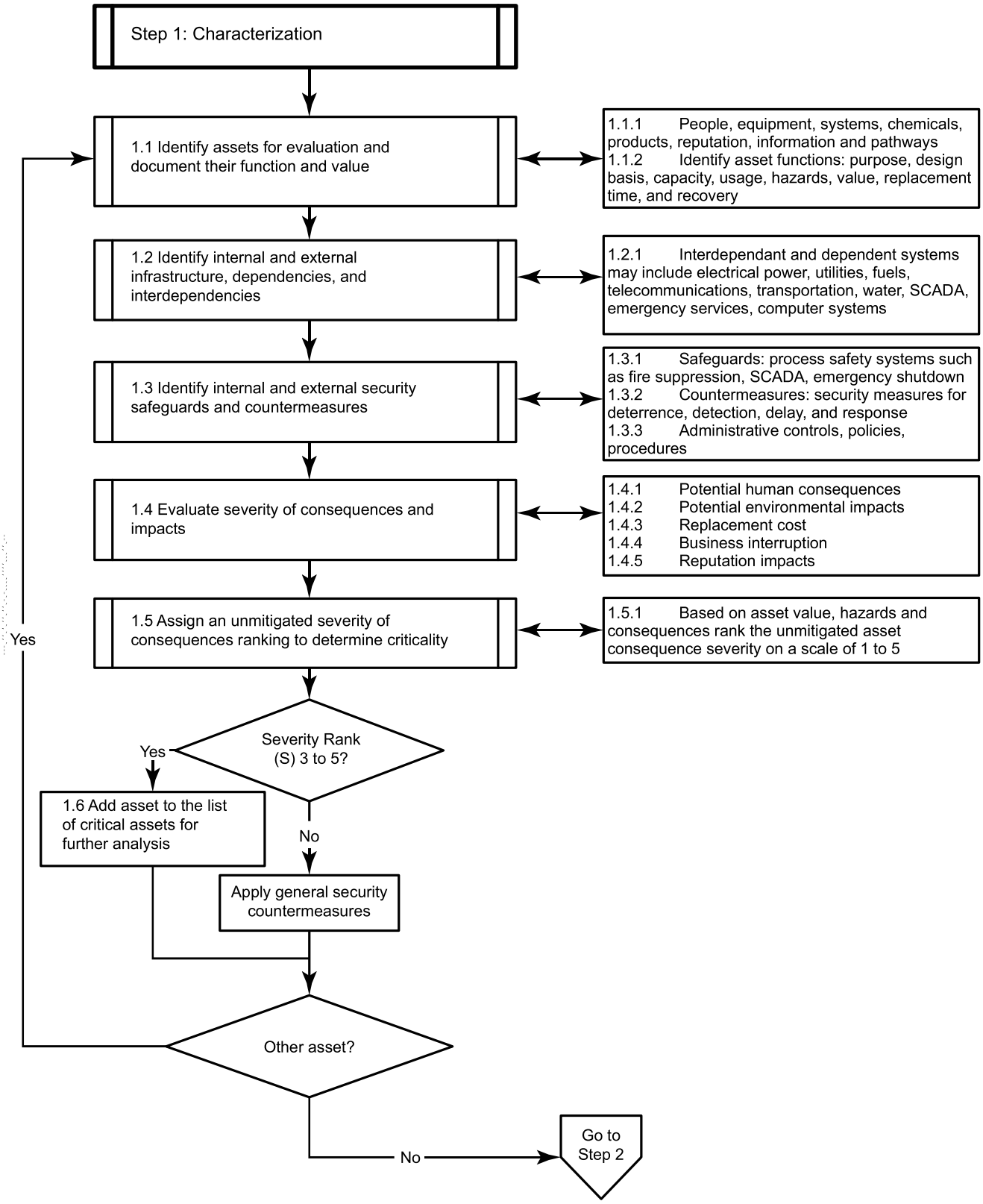

Figure 5—API Security Risk Assessment Methodology—Step 1

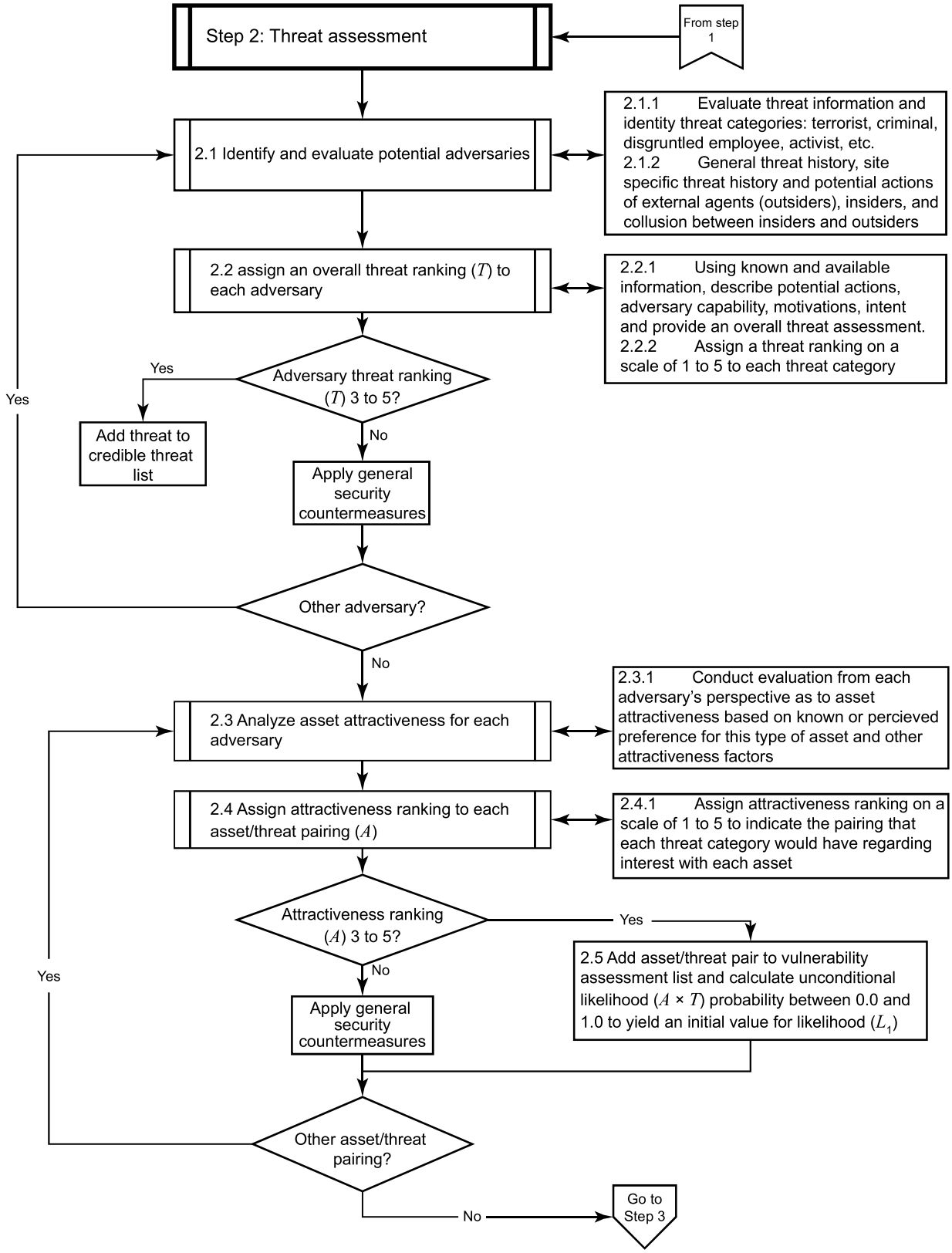

Figure 6—API Security Risk Assessment Methodology—Step 2

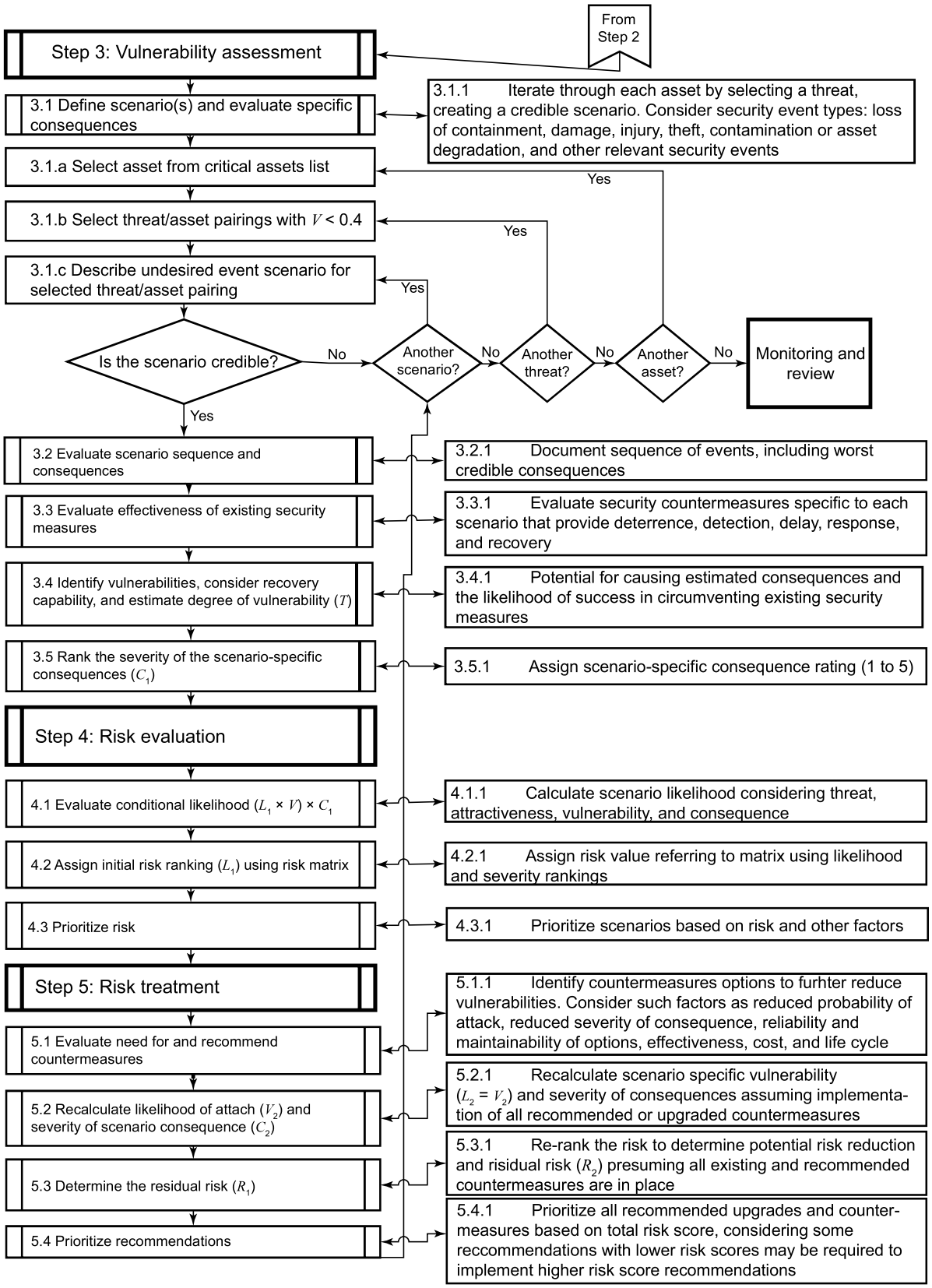

Figure 7—API Security Risk Assessment Methodology—Steps 3 to 5

6.2 Planning for Conducting a SRA

Prior to conducting the SRA team-based sessions, the following activities should be done to ensure a well-planned, effective, and efficient analysis:

— plan the activity well in advance,

— obtain the full support and authorization of management to proceed,

— verify the supporting study data as complete,

— set the objectives and scope of the assessment,

— designate a team knowledgeable of and experienced in the process they are reviewing,

— designate a team leader knowledgeable and experienced in the SRA process methodology.

Prerequisites to conducting the SRA should 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.

6.3 SRA Team

The SRA must be conducted by a team including a core representative group of subject matter experts plus other internal and external participants, if needed. The team shall participate in all steps of the process including the identification of potential security related events or conditions, evaluating the consequences of those events, and determining the need for and means of risk reduction activities for the operator's system. The team members should draw on the years of experience, practical knowledge, and observations from appropriate field operations and maintenance personnel in order to most fully understand where the security risks may reside and what can be done to mitigate them.

The team may consist of personnel from internal company groups representing security, risk management, operations, engineering, safety, environmental, regulatory compliance, logistics/distribution, legal, information technology (IT), control system security, and other employees and contractors as appropriate. This group of experts should focus on the vulnerabilities that degrade the effectiveness of the current facility security plan, with a goal of making recommendations that will enhance an updated facility security plan. The primary purpose of this group is to capture and build into the SRA method the experience of this diverse group of individual experts so that the SRA process will capture and incorporate information that may not be available in typical operator databases.

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

A core team dedicated to the task shall be formed and led by a team leader. Other part-time team members, interviewees, and guests may be used as required for efficiency and completeness. At a minimum, SRA teams should possess the knowledge and/or skills listed in Figure 8. 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. Local law enforcement and first responders can be consulted for advice.

The SRA 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 shall be knowledgeable and experienced in the SRA approach.

API SRA Methodology
The SRA core team members should have the following skill sets and experience as required. — *Team Leader*—Knowledge of and experience with the SRA methodology (not necessarily the most experienced security person). — *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 and emergency response capabilities and procedures. — *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.
The SRA optional or part-time team may include members with the following skill sets and experience as required. — *Security Specialist*—Knowledge of threat assessment, terrorism, weapons, targeting and insurgency/guerilla warfare, or specialized knowledge of detection technologies or other available countermeasures. — *Cyber Security Specialist*—Knowledge of cyber security practices and technologies, IT networks, control systems and business systems. — 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. — *Human Resources*—Knowledge of business employment practices for background checks, contracting, or procurement.

Figure 8—API SRA team Members

6.4 SRA Objectives and Scope

The SRA team leader should develop an objectives and scope statement for the SRA. This helps to focus the SRA and ensure completeness. An example SRA objectives statement is shown in Figure 9.

To conduct an analysis to identify the security risk from internal threats faced by a facility that handles hazardous materials, and to evaluate the countermeasures that are necessary to provide for the protection of the public, the workers, the national interests, the environment, and the company.

Figure 9—SRA Sample Objectives Statement

A work plan should then be developed to conduct the SRA with a goal of achieving the stated objectives. The work plan needs to include the scope of the effort, including which physical or cyber facilities and issues will be addressed. If the study includes consideration of terrorist threats, the key concerns are the intentional misuse of petroleum and hazardous materials that may result in catastrophic consequences caused by malevolent acts. For the API SRA methodology, the key events and consequences of interest that shall be considered include the four event types (Types 1 through 4) listed in Table 1, which are similar to those described as key security events in the Center for Chemical Process Safety security vulnerability analysis guidelines. Other events (Type 5) may be included in the scope, but the study shall address at a minimum the four primary security events (as applicable) since these are the types of events that primarily involve the processes that make petroleum industry facilities unique.

Table 1—Security Events of Concern

API SRA Methodology	
Security Event Type	**Candidate Critical Assets**
Loss of containment or release, damage, or injury.	For facilities handing hazardous substances, loss of containment from the plant site through 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 direct or indirect injury to personnel and the public.
Theft.	Material, asset, or information theft or misuse with the intent to cause harm at the facility or off site or for economic gain.
Contamination (sabotage).	Contamination or spoilage of plant products or information in order to cause worker or public harm on-site or off site or resulting financial damages.
Degradation of assets.	Degradation of assets or infrastructure, or the business function or value of the facility or the entire company, such as destruction of assets for economic disruption or cyber-attack for denial of service.
Other security events (as determined to be relevant).	Reputational attack, cyber-attack, workplace violence, violent crime, sabotage, activist events, theft, vandalism, other crimes relevant to the operation.

6.5 Information Gathering, Review, and Integration

The objective of this step is to provide a systematic methodology for owners/operators to obtain the data needed to manage the security of the facility. Most owners/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.

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.

6.6 Sources of Information

The first step in gathering information is to identify the sources of data needed for conducting the SRA. The team leader shall ensure that appropriate and accurate data sources are used. These sources may be divided into four different classes.

1) *Facility Records*—Facility records or experienced personnel are used to identify the critical areas and other facilities that may either 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, such as population centers and industrial and government facilities.

2) *System Information*—This information identifies the specific function of the various processes and their criticality. System information is analyzed from the 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 important in determining those assets and resources available in-house that are needed to develop and complete a security plan. Information is also needed on those systems that could support a security plan, such as an integrity management program and IT security functions.

3) *Operation Records*—Operating data are used to identify personnel movements and locations, products transported, and the operations pertaining to security issues related to facilities and pipeline segments that may be impacted by security risks. This information is needed to prioritize facilities and pipeline segments for security measures (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*—Information is needed for each facility or pipeline segment in order to determine the level of outside support needed and expected for the security measures to be employed at that facility or pipeline segment. Data are also needed to understand the expectations of the regulatory bodies at the federal, state, and local levels for security preparedness and coordination. Data should also be developed on communication and other infrastructure issues, as well as on sources of information regarding security threats (e.g. information sharing and analysis centers).

6.7 Identifying Information Needs

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

6.8 Locating Required Information

Facility data and information are available in different forms and formats. They may not all be physically stored and updated at one location based on the current use or need for the information. The team should make a list of, and locate, all data required for SRA. Data and information sources may include:

— organizational charts;

— site security plans;

— regulatory requirements for security;

— facility plot plans, equipment layouts, and area maps;

— process and instrument drawings;

— pipeline alignment drawings;

— existing company standards and security best practices;

— product throughput and product parameters;

— emergency response procedures;

— company personnel interviews;

— national, regional, and local emergency response plans;

— law enforcement agency response plans;

— historical security incident reviews;

— support infrastructure reviews;

— regulatory authorities and federal, state, and local agencies;

— intelligence gathered formally or informally;

— previous SRAs;

— threat assessments.

A representative list of supporting data requirements is provided in Annex B. Information security and data protection should be considered when documenting and sharing the information from SRAs. The concepts of “need to share” and securing information adequately from physical and cyber compromise should be exercised.

6.9 Information Collection and Review

The team should ensure that the data and intelligence gathered as a basis for the study is accurate and complete. When data of suspect quality or consistency are encountered, such data should be noted to be updated and so that during the assessment process appropriate confidence interval weightings can be developed to account for these concerns.

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

6.10 Analyzing Previous Incidents

Any previous security incidents relevant to the SRA 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 the facility.

6.11 Conducting a Site Inspection

Prior to conducting the SRA sessions, the team should conduct a site inspection to visualize the facility and to gain valuable insights to the layout, lighting, neighboring area conditions, and other factors that may help to understand the facility and identify vulnerabilities.

6.12 Gathering Threat Information

The team should gather and analyze relevant threat information and other intelligence such as that available from national, state, regional, and local law enforcement agencies.

6.13 Steps of the API SRA—Step 1: Characterization

6.13.1 General

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 are analyzed. The focus is on processes that 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 security countermeasures versus those that require more specific security countermeasures. Through this screening process the team shall produce a list of assets that need to be considered in the analysis. The assets may be processes, operations, personnel, or any other asset. Table 2 summarizes the key steps and tasks required for Step 1.

6.13.2 Step 1.1—Identify Assets

The SRA team shall identify assets for the study. Any asset that is within the scope of the analysis may be considered. For example, the process control system may be designated as critical since its protection from physical and cyber-attack may be important to prevent a catastrophic release or other security event. Table 3 shows 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 nonmaterial elements that enable a facility to operate.

Table 2—Description of Step 1 and Substeps

API SRA Methodology—Step 1: Characterization	
Step	**Tasks**
1.1 Identify assets for evaluation, and document their function and value.	Identify assets of the facility or operation including people, equipment, systems, chemicals, products, and information. This is a higher level assessment to group systems or operations into logical areas or functional objectives in order to organize the study. Document the asset's or operation's purpose (objective), functions (operation), hazards (hazardous properties or outcomes), value (financial or operational worth), and replacement or restoration time (if applicable).
1.2 Identify internal and external infrastructure and dependencies and interdependencies.	Identify the internal and external infrastructures and their dependencies and interdependencies [e.g. electric power, petroleum fuels, natural gas, telecommunications, transportation, water, emergency services, computer systems, air handling systems, fire systems, and supervisory control and data acquisition system (SCADA) systems] that support the operations of each asset. Determine which subassets or other related assets perform or support the functions.
1.3 Identify internal and external security safeguards and countermeasures.	The SRA team identifies and documents the existing security and process safety layers of protection. The team gathers information and develops a general knowledge of the existing countermeasures but does not yet calculate their effectiveness. (The evaluation of their effectiveness is performed during the vulnerability analysis step.)
1.4 Evaluate severity of consequences and impacts.	Evaluate the hazards, consequences, and/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 (assuming a complete loss for any reason, i.e. worst credible case).
1.5 Assign an initial severity of consequence without consideration of any existing countermeasures ranking (C) to determine criticality.	Rank the highest of each of the consequence criteria to develop a maximum initial severity of consequence without consideration of any existing countermeasures for each asset or function. For risk-based prioritization of effort, it can be useful to screen using: if C = 3 to 5, then add asset to the critical asset list; if C = 1 to 2, then add asset to the general asset list and make further study of the scenario optional.
1.6 Identify the list of "critical assets" for further analysis.	Based on the C ranking from 1.5 above, develop a refined list of "critical assets" for further study.

The following types of information should be considered by the SRA team as appropriate for making a determination of applicability as a "critical asset" where hazardous chemical assets are involved.

— Any chemical in Appendix A ("DHS Chemicals for Interest") of the U.S. Department of Homeland Security's (DHS) *Chemical Facility Anti-terrorism Standards* (6 *CFR* Part 27) or other applicable chemical security regulatory requirement.

— Any applicable regulatory lists of highly hazardous chemicals, such as the Clean Air Act 112(r) list of flammable and toxic substances for the U.S. Environmental Protection Agency (EPA) risk management program standard 40 *CFR* Part 68 or the U.S. Occupational Safety and Health Administration (OSHA) process safety management standard 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,

  — the Australia Group list of chemical and biological weapons.

— Material destined for the food, nutrition, cosmetic or pharmaceutical chains.

— Chemicals that are susceptible to reactive chemistry.

— Economically critical chemicals.

Table 3—Example List of Candidates to be Considered as Critical Assets

API SRA Methodology	
Security Event Type	**Candidate Critical Assets**
Loss of containment, damage, or injury.	— The public, employees, contractors, and visitors. — Process equipment handling hazardous chemicals, including processes, pipelines, and storage tanks. Marine vessels and facilities, pipelines, and other transportation systems.
Theft.	— Hazardous 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. — Important economic assets ranging from intellectual property to physical assets.
Contamination.	— Raw material, intermediates, catalysts, products, processes, storage tanks, and pipelines. — Critical business or process data.
Degradation of assets.	— Processes containing hazardous chemicals. — Business image and community reputation. — Utilities (electric power, steam, water, natural gas, and specialty gases). — Telecommunications systems. — Business systems.
Other security events (determined to be relevant).	— Corporate identity and reputation and related value. — Personnel. — Critical data. — Operational integrity. — Records.

The SRA team 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;

— employees, contractors, or visitors;

— critical infrastructure and support utilities.

Document the asset's or operation's purpose (objective), functions (operation), hazards (hazardous properties or outcomes), value (financial or operational worth), and replacement or restoration time (if applicable). The SRA team shall clearly identify the functions of the assets, such as "provides power to the crude unit" or "is the IT server housing all business records."

6.13.3 Step 1.2—Identify Internal and External Infrastructure and Dependencies

The SRA team shall identify the 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, or the steam power plant is the sole source of steam supply for the refinery.

6.13.4 Step 1.3—Identify Internal and External Safeguards and Countermeasures

The SRA 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.

6.13.5 Step 1.4—Evaluate Severity of Consequences and Impacts

This step includes the determination of the specific consequences of a loss. The SRA team should consider relevant chemical use and hazard information, as well as information about the facility. The team should then 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 security incidents that can result in serious consequences such as fire, explosion, toxic release, radioactive exposure, and environmental contamination, such as shown in Table 4.

Table 4—Possible Consequences of SRA Security Events by Threat Agent

API SRA Methodology				
Possible Consequences	**Terrorist**	**Criminal**	**Disgruntled Insider**	**Activist**
Public fatalities or injuries.	X	—	—	—
Site personnel fatalities or injuries.	X	—	X	X
Workplace violence.	—	—	X	—
Theft or release of chemicals.	X	X	X	—
Disruption to national economy.	X	—	—	X
Disruption of company operations.	X	X	X	X
Financial loss.	X	X	X	X
Environmental damage.	X	—	X	—
Loss of, or damage to, critical data.	X	X	X	X
Damage to reputation or business viability.	X	X	X	X

The consequence analysis may be done in a general manner by using the team's judgment to determine credible outcomes of the event should it be successful. The consequences of a security event at a facility should be expressed in terms of the degree of expected acute health effects (e.g. fatality, injury), property damage, environmental effects, etc. should the scenario occur. This definition of consequences is similar to that used for accidental releases and so may be integrated with safety risk assessment scales as is appropriate for security-related events. The key difference is that consequences may involve effects that are more severe than those expected with accidental risk and the likelihood of the act is based on human actions of malfeasance, which may be less predictable.

The specific consequences of each scenario shall be documented. Team members should review any off-site consequence analysis data previously developed for safety analysis purposes or prepared for security analysis as a basis of the assessment. 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 may be a major influence on the threat's selection of a target, and on the person(s) seeking to protect that target. In terms of attractiveness to a terrorist, a target that could expose a large number of persons is likely to be a high-value, high-payoff target.

6.13.6 Step 1.5—Assign Consequence Ranking (C) to Determine Criticality

A risk ranking matrix shall be used to rank the degree of severity. The risk matrix and associated definitions may be defined by the user. Table 5 illustrates a set of example consequence definitions based on five categories of events:

a) fatalities and injuries,

b) environmental impacts,

c) property damage,

d) business interruption,

e) damage to reputation or negative publicity.

Table 5—Example Definitions of Consequences of the Event

API SRA Methodology	
Description	**Ranking**
a) Possibility of minor injury on-site; no fatalities or injuries anticipated off site. b) No environmental impacts. c) Up to $X loss in property damage. d) Very short-term (up to X weeks) business interruption/expense. e) Very low or no impact or loss of reputation or business viability; mentioned in local press.	1
a) On-site injuries that are not widespread but only in the vicinity of the incident location; no fatalities or injuries anticipated off site. b) Minor environmental impacts to immediate incident site area only, less than X year(s) to recover. c) $X to $X loss in property damage. d) Short-term (>X week to Y months) business interruption/expense. e) Low loss of reputation or business viability; query by regulatory agency; significant local press coverage.	2
a) Possibility of widespread on-site serious injuries; no fatalities or injuries anticipated off site. b) Environmental impact on-site and/or minor off-site impact, Y year(s) to recover. c) Over $X to $X loss in property damage. d) Medium-term (Y to Z months) business interruption/expense. e) Medium loss of reputation or business viability; attention of regulatory agencies; national press coverage.	3
a) Possibility of X to Y on-site fatalities; possibility of off-site injuries. b) Very large environmental impact on-site and/or large off-site impact, between Y and Z years to recover. c) Over $X to $X loss in property damage. d) Long-term (X to Y years) business interruption/expense. e) High loss of reputation or business viability; prosecution by regulator; extensive national press coverage.	4
a) Possibility of any off-site fatalities from large-scale toxic or flammable release; possibility of multiple on-site fatalities. b) Major environmental impact on-site and/or off site (e.g. large-scale toxic contamination of public waterway), more than XX years/poor chance of recovery. c) Over $X loss in 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. e) Very high loss of reputation or business viability; international press coverage.	5

The user shall define a risk matrix that includes those categories at a minimum. The risk matrix may use a scale that includes more or fewer levels of severity than the five included in Table 5. The formulas used in the methodology, scales, and risk matrix including definitions of likelihood and consequence shall be defined by the user. The recommended API SRA risk matrix is based on a scale of 1 to 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 as a candidate to be considered for inclusion in the critical asset list. The attractiveness of the asset will later be used for further screening of critical assets.

6.13.7 Step 1.6—Select the Most Critical Assets for Further Analysis

The criticality of each identified asset shall be designated. 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, potential for the misuse of the material to produce a weapon, or the physical properties of the material to contaminate a public resource. The SRA 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 shall be paired with specific threats and evaluated against the potential types of attack that could occur.

6.14 Steps of the API SRA—Step 2: Threat Assessment

6.14.1 General

The threat assessment step involves the substeps shown in Table 6.

6.14.2 Step 2.1—Identify and Evaluate Potential Threats

The next step is to identify specific classes of adversaries that may perpetrate the security-related act. The threat characterization substep is done by developing as complete an understanding as is possible of the threat history, capabilities, and intent. A threat analysis shall be performed to pair the assets with each threat class.

Depending on the threat, users shall determine the types of potential security incidents and, if specific information (intelligence) is available on potential targets and the likelihood of an act, specific countermeasures may be taken. Information may be too vague to be useful, but SRA teams should seek available information from federal, state, and local law enforcement officials in analyzing threats. Absent specific threat information, the SRA 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 in order to properly respond to those threats. This section describes a threat assessment approach as part of the security management process.

A threat assessment is used to evaluate the likelihood of threat 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 performed systematically and kept current in order to be useful. The determination of the threats posed by different adversaries leads to the recognition of vulnerabilities and to the evaluation of countermeasures required to manage the threats. Without a situation-specific threat in mind, a company cannot effectively develop a cost-effective security management system. If threats change, the assumptions in the SRA may no longer be valid.

Table 6—Description of Step 2 and Substeps

API SRA Methodology—Step 2: Threat Assessment	
Step	**Tasks**
2.1 Identify and evaluate potential threat.	Evaluate threat information and identify threat categories and potential adversaries. Identify general threat categories. Consider threats posed by internal, external sources, and collusion between internal and external sources.
2.2 Assign threat ranking to threat.	Evaluate each threat and provide an overall threat assessment and ranking for each threat by using all known or available information. Consider such factors as the general nature/history of threat; specific threat experience/history of the facility/operation; known capabilities/methods/weapons; and potential actions and intent/motivation of threat. — If T = 3 to 5, then add to credible threats. [a] — If T = 1 or 2, the optional to discuss or add to general discussion or dismiss from analysis.
2.3 Analyze asset attractiveness for each threat.	Conduct an evaluation, from the threat perspective, of potential asset attractiveness for those assets identified in Step 1.
2.4 Assign an attractiveness ranking for each asset-threat pairing.	Assign an attractiveness ranking (A) to each asset-threat pair. — If A = 3 to 5, then add to credible asset/threat pairings (targets). [b] — If A =1 or 2, then add to general threats or dismiss.
2.5 Calculate unconditional likelihood (L_1).	Multiply the threat (T) ranking by the attractiveness (A) ranking, each expressed as a value of 1 to 5 (reflecting a corresponding conditional probability between 0.0 and 1.0 that a particular threat will be attracted to a particular asset) to yield an initial value for likelihood (L_1).

[a] The criterion is subject to correlation to the specific risk matrix and risk tolerance of the user. The user can adopt other criteria for screening threats.

[b] The criterion is subject to correlation to the specific risk matrix and risk tolerance of the user. The user can adopt other criteria for screening attractiveness.

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

Some threats are assumed to be continuous, whereas others are assumed to be variable. Depending on the threat level, different security measures beyond 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 threat groups. No matter how much is known about potential threats, it may not be possible to identify every threat or to ensure that complete information is available about the threats. Consequently, a threat assessment should be accompanied by a vulnerability assessment to provide better assurance of preparedness for a terrorist or other threat attack.

Threat information gathered by both the intelligence and law enforcement communities may 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, possibly including terrorism.

Threats shall be considered from internal and external threats or a combination of those adversaries working in collusion. Insiders are defined as those individuals who normally have authorized access to the asset. They may pose a particularly difficult threat because of their training, knowledge of the facilities, the possibility for deceit or deception, and their unsupervised access to critical information and assets.

The threat categories that shall be considered are those that include intent and capability of causing harm to the facilities and to the public or environment within the scope of this standard and the objectives of the study. Typical threats that may be included in a SRA are: international terrorists, domestic terrorists (including disgruntled individuals/"lone wolf" sympathizers), disgruntled personnel, criminals, or extreme activists.

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. The user can take the approach to make an assumption that the threat likelihood for higher order (e.g. terrorist) threats is a given level (perhaps "unity", i.e. an act will occur) at the facility level for every location that has adequate attractiveness to that threat. Site-specific information will adjust the critical asset rankings accordingly.

To be effective, threat assessment should be considered a dynamic process, whereby the threats are continuously evaluated for change. During any given SRA exercise, the threat assessment shall be referred to for guidance on general or specific threats facing the assets. The company's threat assessment should be regularly reviewed and updated as required given additional information and analysis of vulnerabilities.

Threat acts may be perpetrated by insiders, outsiders, or a combination of the two. Insiders are those personnel that have routine, unescorted access to areas where outsiders are not allowed without escort. Collusion between the two may be the result of monetary incentive, ideological sympathy, or coercion.

The threat characterization will assist in evaluating the issues associated with insider, outsider, and colluding threats. The SRA team shall consider each type of threat identified as credible, generally define their capabilities and motivation, and determine the credibility of each threat for the specific facility or operation being analyzed.

6.14.3 Step 2.2—Assign Threat Ranking to Threat

Table 7 depicts the five-level ranking system for defining threat rankings against an asset.

Table 7—Threat Ranking Criteria

API SRA Methodology	
Threat Level	**Description [a]**
1—Very low	Indicates little or no credible evidence of capability or intent and no history of actual or planned threats against the asset or similar assets (e.g. "no expected attack in the life of the facility's operation").
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 asset (e.g. "≥ 1 event is possible in the life of the facility's operation").
3—Medium	indicates that there is a possible threat to the asset or similar assets based on the threat's desire to compromise similar assets, but no specific threat exists for the facility or asset (e.g. "≥ 1 event in 10 years of the facility's operation").
4—High	Indicates that a credible threat exists against the asset or similar assets based on knowledge of the threat's capability and intent to attack the asset or similar assets, and some indication exists of the threat specific to the company, facility, or asset (e.g. "≥ 1 event in 5 years of the facility's operation").
5—Very high	Indicates that a credible threat exists against the asset or similar assets; that the threat demonstrates the capability and intent to launch an attack; that the subject asset or similar assets are targeted or attacked on a frequently recurring basis; and that the frequency of an attack over the life of the asset is very high (e.g. "1 event/event per year").

[a] User defined values should be applied.

6.14.4 Step 2.3—Analyze Asset Attractiveness

The asset attractiveness ranking shall be assigned by the team. There may be a need to predefine an internal process to resolve disputes and seek agreement within the team as this is a consensus process. The attractiveness of the target to the threat is a key factor in determining the likelihood of an attack. Examples of issues that may be addressed here include the following.

— Value of asset to the adversary (theft or damage for personal gain, noneconomic factors such as damaging the company reputation or brand, obtaining, or damaging a prized iconic or symbolic target).

— For chemical theft, usefulness of the chemical as a weapon or to cause collateral damage (whether it is a chemical or biological weapons precursor chemical or explosive, toxic, or flammable material that can be weaponized).

— Difficulty of the act, including ease of access and degree of existing security measures (soft target vs hardened target).

— Recognition of the target while staging an act or while in the process of the act (ease of identifying the target).

— Proximity to a symbolic or iconic target, such as a national landmark (possible terrorist or activist objective).

— Unusually high corporate profile among possible activists, such as a major company with high visibility working in a particular environment.

— Any other variable not addressed elsewhere, when the SRA team agrees it has an impact on the site's value as a target or on the potential consequences of an attack.

— The asset chosen provides the most vulnerable target that achieves the objective of the threat, and where the threat believes it will have the highest level of success.

The SRA team should use the best judgment of its subject matter experts to assess attractiveness. Each asset shall be analyzed to determine the factors that might make it a more or less attractive target to the threat, and the information documented.

Asset attractiveness is an assessment of the target's value from the threat's perspective and is one factor used to determine likelihood of the act being committed. The attractiveness of assets varies with the threat and its motivation, intent, and capabilities. For example, the threat posed by an international terrorist group and the assets in which it might be interested may be quite different from the assets of interest to an activist, a disgruntled individual, or a criminal. In the case of a SRA where the initiating threat is a natural event, such as a hurricane or flood, and the team is analyzing the security events that may result from this situation, the attractiveness factor could be based on susceptibility of assets to the threat.

The SRA team shall rank the attractiveness factor for each critical asset to each credible threat by using the scale shown in Table 8 or equivalent.

6.15 Steps of the API SRA—Step 3: Vulnerability Assessment

6.15.1 General

The vulnerability assessment step involves five steps, as shown in Table 9. Once the SRA team has determined why an event can be induced, it shall determine how that threat could succeed by conducting the following substeps.

Table 8—Target Attractiveness Ranking Definition

API SRA Methodology			
Ranking Level	**Descriptor**	**Conditional Probability of the Act**	**Threat Ranking**
1	Very low	0.0 to 0.2	Threat would have little to no level of interest in the asset.
2	Low	>0.2 to 0.4	Threat would have some degree of interest in the asset, but it is not likely to be of interest compared to other assets.
3	Medium	>0.4 to 0.6	Threat would have a moderate degree of interest in the asset relative to other assets.
4	High	>0.6 to 0.8	Threat would have a high degree of interest in the asset relative to other assets.
5	Very high	>0.8 to 1.0	Threat would have a very high degree of interest in the asset, and it is a preferred choice relative to other assets.

Table 9—Description of Step 3 and Substeps

API SRA Methodology—Step 3: Vulnerability Assessment	
Step	**Tasks**
3.1 Define scenarios and evaluate specific consequences.	The team shall use scenario analysis to document the threat's potential acts against an asset including the following. 1) Select asset from critical asset list, with a threat/attractiveness rating of medium to very high. 2) Select an event type (e.g. unauthorized access, loss of containment, theft, etc.). 3) Identify the threat and the threat type (internal, external, colluded threat), then import the threat (T) and attractiveness (A) calculations that yielded likelihood (L_1) from Step 2. 4) Describe the security scenario for the assumed threat and asset pairing.
3.2 Evaluate act sequence and potential consequences (C_1).	Document the sequence of events including worst credible scenario-specific consequences C_1 with consideration of existing safeguards to identify the worst credible outcome if the act is successful.
3.3 Evaluate effectiveness of existing security measures.	Identify the existing measures intended to protect the assets and estimate their levels of effectiveness in reducing the vulnerabilities of each asset to each threat. Consider the security objectives of deter, detect, delay, respond, and recover and such strategies as defense in depth and balanced security when evaluating presence of countermeasures.
3.4 Identify vulnerabilities, considering recovery capability, and estimate degree of vulnerability.	Identify the potential vulnerabilities of each asset to applicable threats. Estimate the degree of vulnerability of each asset for each assumed act or incident and thus each applicable threat. Identify the means available to recover or continue operations through such resiliency practices as redundancy, shifting of operations, alternate supply, etc. and determine whether these factors would reduce the vulnerability to the specific scenario being evaluated. The vulnerability (V) of the asset is $V = L_2$ represents a surrogate for the conditional probability of success of the event.
3.5 Rank the severity of scenario-specific consequence (C_2 = mitigated consequences).	Evaluate the consequences specific to the scenario, which may be lower than the maximum identified in the asset criticality assessment since this is scenario-specific or may be higher if it is recognized that collateral damage yields a consequence greater than for the previous assumption.

6.15.2 Step 3.1—Define Scenarios

The team shall define scenarios that assume specific acts and the means by which the threat may attempt the assumed acts against each asset, identify the threat and the threat type (internal, external, colluded threat), then import the threat (T) and attractiveness (A) calculations that yielded likelihood (L_1) from Step 2.5. Describe the security scenario for the assumed threat and asset pairing.

The individual assets are evaluated case by case, but the user can also evaluate the perimeter security strategy directly by considering each pathway from the uncontrolled through to the controlled area of the facility. This can be done for ordinary pathways intended for personnel or vehicles (gates and roadways) or directly by breaching the perimeter barrier (cutting of a fence or breaching a vehicle barrier forcefully). For each pathway with an attractiveness ranking from medium through very high (A = 3 to 5, from Step 2), the SRA team should develop a perimeter penetration scenario associated with unauthorized access [1]. The team can assume that successful penetration through that pathway into the site containing the actual critical assets will be assigned the provisional severity of consequence at the same level as the maximum consequence that could be achieved by the threat since they would at this point have access to the asset (even though the pathway itself is not the end objective of the threat it represents the means of accessing the asset). For each asset (or activity) in the list of critical target assets with an unconditional severity consequence (C) of 3 to 5 (from Step 1) and a corresponding attractiveness ranking from medium through very high (from Step 2), the SRA team should select an event type (e.g. loss of containment, theft, disruption of operations, etc.). The SRA team should then identify the threat and the threat type (insider, outsider, collusion) and import the threat (T) and attractiveness (A) calculations that yielded likelihood (L) from Step 2.

6.15.3 Step 3.2—Evaluate Scenario Sequence and Consequences

The SRA team shall then develop credible scenarios to define the potential acts. Once the SRA team has determined how an act can be induced, it shall describe how a threat could reasonably execute the act. The SRA team shall document the general sequence of the act in sufficient detail to allow others reviewing the SRA results to understand the assumptions of the scenario and conclusions. The SRA team shall also deliberate on the level of estimated consequence that each scenario under consideration would reasonably yield.

Sometimes the consequence of the act will exactly match the asset severity ranking from the initial maximum screening estimate in Step 1, but in other scenarios the threat may not be able to obtain the maximum consequence (e.g. a disgruntled insider conducting sabotage would likely have a lower consequence than a terrorist attack); conversely, the postulated scenario may be able to exceed the severity identified in Step 1 because the threat could damage other adjacent assets as collateral damage, the effect of which when aggregated would elevate the severity of the consequence.

6.15.4 Step 3.3—Evaluate Effectiveness of Existing Security Measures

The SRA team shall 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. Guidance is provided in Table 10 on recommended assumptions and rules for assessing adequacy of security layers of protection.

6.15.5 Step 3.4—Identify Vulnerabilities and Estimate Degree of Vulnerability

Vulnerability is any weakness that can be exploited by a threat to gain unauthorized access or the subsequent destruction or theft of an asset. Vulnerabilities can result from, but are not limited to, weaknesses in current management practices, physical/technical/cyber security, or operational security practices. For each asset, the vulnerability or difficulty of attack is considered by using the five-level ranking system defining vulnerability (V). The rankings made by the SRA team may be assigned corresponding values ranging from 1—very low to 5—very high for use in the likelihood calculation. Vulnerability can be expressed as a numeric value of 1 through 5 reflecting a conditional probability for vulnerability of the asset to the attack (as a surrogate for the likelihood of expected attack success expressed as L_2; $L_2 = V$) as shown in Table 11.

[1] The criterion is subject to correlation to the specific risk matrix and risk tolerance of the user. The user can adopt other criteria for screening acts to be considered for perimeter analysis.

Table 10—Layers of Countermeasures Guidance

API SRA Methodology	
Guidance	**Application**
To provide effective security, there should be a robust set or layers of security measures by using concepts of defense in depth and balanced security.	Identify each of the countermeasure or layers of countermeasures applicable to the scenario.
Factors that should be considered for accrediting an existing measure as a countermeasure.	1) Design is fit for purpose, given the scenario. 2) Operational readiness and reliability. 3) Expected effectiveness to accomplish the purpose. 4) Balanced security (no one path or act to access the site is more vulnerable than others or the minimum required). 5) Defense in depth (there are sufficient layers of security than make the likelihood of success sufficiently low).

Table 11—Vulnerability Ranking Criteria

API SRA Methodology			
Vulnerability Level	**Descriptor**	**Conditional Probability of Success**	**Description**
1	Very low	0.0 to 0.2	Indicates that multiple layers of effective security measures to deter, detect, delay, respond to, and recover from the threat exist, and the chance that the adversary would be readily able to succeed at the act is very low.
2	Low	>0.2 to 0.4	Indicates that there are effective security measures in place to deter, detect, delay, respond, and recover; however, at least one weakness exists that a threat would be able to exploit with some effort to evade or defeat the countermeasure.
3	Medium	>0.4 to 0.6	Indicates that although there are some effective security measures in place to deter, detect, delay, respond, and recover, but there is not a complete and effective application of these security strategies and so the asset or the existing countermeasures could still be compromised.
4	High	>0.6 to 0.8	Indicates there are some security measures to deter, detect, delay, respond, and recover, but there is not a complete or effective application of these security strategies and so the adversary could succeed at the act relatively easily.
5	Very high	>0.8 to 1.0	Indicates that there are very ineffective security measures currently in place to deter, detect, delay, respond, and recover, and so the adversary would easily be able to succeed.

6.15.6 Step 3.5—Rank the Severity of Consequence

The SRA team then evaluates the consequences specific to the scenario (mitigated severity), which may be different than the maximum identified in the asset criticality assessment; it may be lower or it may include collateral damage that yields a consequence greater than for the asset alone. The team records the new severity of consequence to yield a value ranging from 1 through 5 for C_1. (C_1 = mitigated severity of consequences.)

6.16 Steps of the API SRA—Step 4: Risk Analysis/Ranking

The next step is to determine the level of risk of the adversary exploiting the asset given the existing security countermeasures. Table 12 lists the substeps.

The scenarios shall be risk-ranked by the SRA team based on a SRA risk matrix similar to that depicted in Figure 10 (the owner/operator can defined their risk matrix for this purpose). The risk matrix should be used to plot the risk of each scenario based on its likelihood (L) and consequences (C). The intent is to categorize the assets into discrete levels of risk so that appropriate countermeasures can be applied to each situation.

Table 12—Description of Step 4 and Substeps

API SRA Methodology—Step 4: Risk Evaluation	
Step	**Tasks**
4.1 Evaluate conditional likelihood ($L_1 \times V$) that includes existing security countermeasures, with the scenario-specific severity of consequence (C_1).	As a function of consequence and probability or frequency of occurrence, determine the relative degree of risk to the facility in terms of the expected effect on each critical asset and the likelihood of a successful attack [a function of the threat or adversary, as evaluated in Step 2 (L_1), multiplied by the degree of vulnerability of the asset as evaluated in Step 3 ($L_2 = V$)] that will achieve the mitigated scenario-specific consequence in Step 3 (C_1).
4.2 Assign risk ranking (R_1) by using risk matrix.	Plot each scenario on the risk matrix based on its likelihood [($L_1 \times L_2$), where $L_2 = V$] and scenario-specific severity of consequence (C_1) to determine the corresponding R value (R_1), which categorizes the scenarios into discrete levels of existing mitigated risk estimates.
4.3 Prioritize risk.	Calculate and prioritize the risks based on the relative degrees of risk and the likelihoods of successful attacks for each scenario. Other factors may be used to prioritize risk as appropriate.

API SRA Methodology

			Likelihood (L)				
			VL	**L**	**M**	**H**	**VH**
			1	**2**	**3**	**4**	**5**
Consequences (C)	**VH**	**5**	3	4	4	5	5
	H	**4**	2	3	4	4	5
	M	**3**	2	2	3	4	4
	L	**2**	1	2	2	3	4
	VL	**1**	1	1	2	2	3
			VL	**L**	**M**	**H**	**VH**
			1	**2**	**3**	**4**	**5**

NOTE For this matrix, a risk ranking of "5" represents the highest risk.

Figure 10—Example Risk Ranking Matrix

6.17 Steps of the API SRA—Step 5: Identify Countermeasures

Countermeasures analyses conducted by the SRA team shall identify gaps between the existing security profile and the desirable level of security where additional recommendations or upgrades may be necessary to reduce risk to more acceptable levels. In assessing the need for additional countermeasures, the user shall consider the following countermeasures strategies for each scenario.

— *Deter*—Deter an attack if possible, or substitute inherently safer technologies to reduce target attractiveness or consequences.

— *Detect*—Increase ability to detect an attack.

— *Delay*—Increase barriers to delay the attacker until responders can intervene and increase the likelihood of detection.

— *Respond*—Increase the speed, number, or effectiveness to respond to neutralize the adversary, control a release, evacuate or shelter in place, or other actions to reduce the likelihood of a successful attack.

— *Recover*—Improve ability to recover from an incident, or improve continuity of operations through increased resiliency.

The SRA team shall evaluate the merits of effectiveness of additional countermeasures by listing them and estimating their net effect on the lowering of the likelihood or severity of the attack. The SRA team shall attempt to lower the risk of each scenario to acceptable levels based on the company's risk tolerance. Table 13 lists the substeps.

Table 13—Description of Step 5 and Substeps

API SRA Methodology—Step 5: Risk Mitigation	
Step	**Tasks**
5.1 Evaluate need for and recommend countermeasures if necessary.	The team shall Identify countermeasures options to further reduce the vulnerabilities (and thus the risks) while considering such factors as: — reduced probability of successful attack, — reduced severity of consequence, — the reliability and maintainability of the options, — the capabilities and effectiveness of mitigation options, — the costs of mitigation options, — the feasibility and functional life cycle of the options.
5.2 Recalculate likelihood of attack (V_2) and severity of scenario consequence (C_2).	The team shall recalculate scenario-specific likelihood (V_2), which also includes the initial threat/attractiveness pairing calculation for L_1, and any revised severity of consequence (C_2), based on the expectation that all recommended upgrades and countermeasures will be implemented. The team should consider that reduction in severity of consequence rarely occurs and only then when one or more of the recommended new countermeasures demonstrably changes the hazard or severity of the loss such as when the process or other asset itself has been modified. An example is when a blast resistant building is constructed that protects the operators hence loss of life is reduced or when an asset is reduced in importance or hazard potential.
5.3 Determine residual risk (R_2).	The team shall re-rank the risk to determine potential risk reduction and residual risk (R_2), presuming that all recommended upgrades are implemented.
5.4 Prioritize recommendations.	The team should prioritize recommended upgrades and countermeasures based on such factors as the total risk score (the number of times throughout all scenarios that each recommendation is listed as a requirement for reducing risk) and prepare ordered recommendations for the decision makers. Take into consideration that some recommendations with lower risk scores may be required in order to implement other recommendations that have higher risk scores (e.g. lower-risk-score lighting upgrades may be required in order to ensure that higher-risk-score CCTV installations operate efficiently). Other factors may be used to prioritize risk as appropriate.

6.18 Summary of Approach

A summary of approach is as follows.

a) Identify and characterize assets (assets or activities, pathways through the perimeter to the assets), document key aspects of their purpose, design basis, dependencies/interdependencies.

b) Document possible threats and discuss their history, capabilities, motivation, and other threat factors and assign a threat ranking (T) on a scale of 1 to 5 to determine if the threat is credible. Credible may be defined by the user—for example, those threats with rankings of 3 to 5.

c) Conduct an attractiveness assessment for all credible threats and assign attractiveness ranking (A) on a scale of 1 to 5 to each asset, activity, or pathway. Attractive assets may be defined by the user—for example, those assets with attractiveness rankings of 3 to 5.

d) Consider any asset that is both credible and attractive per steps above to be a critical target; pair each critical target asset with related threats and develop potential scenarios to represent possible acts in line with the threat assessment and the particular asset in question.

e) Assuming the act is successful, determine potential worst credible consequences and conduct a vulnerability analysis and risk assessment of existing mitigated risk (R_1).

For each scenario, perform the following.

1) Determine security event type (categories of security events could be degradation of the asset, theft or diversion, criminal activity, activism, etc.).

2) Identify potential threat type (terrorist, criminal, etc.) and category (internal, external, and colluded).

3) Rank specific threat (T) for each scenario (T = 1 to 5).

4) Evaluate specific attractiveness (A) to the scenario and multiply A (on a scale of 0.0 to 1.0) $\times$ T for the scenario to derive an estimate of likelihood of security event occurring (L_1) expressed on a scale of 1 to 5 (rounded up to a whole integer).

$$L_1 = A \times T$$

5) Identify existing security countermeasures for the scenario (evaluate if there are layers of security and reliable means to deter, detect, delay, respond, and recover).

6) Identify vulnerabilities (gaps between existing safeguards and necessary countermeasures that allow a scenario to occur or increase the likelihood of success of the threat to commit the act) and evaluate what specific gaps there are in the layers of security and means to deter, detect, delay, respond, and recover.

7) Determine vulnerability ranking (V) including consideration of the likelihood of the existing countermeasures allowing the act to occur; $V = L_2$, expressed as a value from 1 to 5.

$$L_2 = V$$

8) Determine the scenario-specific severity of consequences (C_1).

9) Determine existing mitigated risk ranking (R_1). R_1 is a function of the product of the threat multiplied by the attractiveness of the target, multiplied by the vulnerability of the target to the act described by the scenario

[$(T \times A) \times V$, or $(L_1 \times L_2)$] and must also include consideration of the scenario-specific severity of consequences (C_1).

$$R_1 = (C_1, L_1 \times V)$$

10) Plot the scenario mitigated risk ranking (R_1) on the risk matrix, where the likelihood calculation ($L_1 \times L_2$) is plotted on the likelihood axis as a value from 1 to 5 and severity of consequence is plotted on the severity axis as a value from 1 to 5.

f) Conduct consequence and vulnerability analysis and SRA of residual risk (R_2) as follows.

1) Identify any recommended countermeasures that address each existing mitigated risk (R_1) as required.

2) Derive residual risk (R_2). For each R_1, estimate the reduction in risk based on aggregate recommended countermeasures by recalculating the scenario-specific likelihood (V_2) and the scenario-specific severity of consequences (C_2), based on the expectation that all new recommended countermeasures will be implemented.

g) Prioritize recommendations. Evaluate countermeasures by using the numeric value from the numbered matrix. As a guideline to help the SRA team establish the order of priority, assign “high” risks as the highest priority and then add the middle zone risks.

h) Sequentially bundle similar recommendations. When there are “lower priority” recommendations of a very similar nature to a recommended type of “higher priority” countermeasure (i.e. CCTV, access control system, protective force), group the recommendations together under the higher priority recommendation (i.e. denoting them as “2.1,” “2.2,” “2.3,” etc.). This permits the collection of similar elements that are sequential in nature or that may need to be considered together as a package when conducting cost-benefit calculations).

Range critical assets in order of risk reduction, from those providing the greatest to those providing the least reduction, by comparing R_1 to R_2. For each asset, include the threat category and related scenario, identify the related recommendations in order by priority, and state the anticipated reduction in risk.

6.19 Follow-up to the SRA

A completed SRA shall be documented in a written report that includes:

— the dates the SRA was performed;

— a roster of the SRA team members, including their roles and responsibilities within the study;

— a description of the scope and objectives of the study;

— a description of, or reference to, the SRA methodology used for the study;

— the documented list of assets identified;

— the determination of critical assets and the basis for each determination;

— the threat assessment;

— the attractiveness analysis;

— the documentation of plausible acts;

— the identification of security vulnerabilities;

— an evaluation of existing countermeasures against each act;

— the risk ranking (R_1) related to each applicable scenario;

— a set of recommendations to reduce risk (as necessary);

— risk ranking subsequent to implementation of all recommended upgrades, reflecting the residual risk once all recommendations have been implemented (R_2);

— prioritization of recommended upgrades, in order based on risk reduction (optional).

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

Annex A
(informative)

Forms and Worksheets

A.1 Form 1—Characterization Form

Determine the major assets of the facility including process units, control rooms, tankage, truck and rail bays, marine loading or unloading points, communications networks, pipeline manifolds, utilities, and supporting infrastructure (e.g. motor control centers, vapor recovery units, raw water intake, electrical power, process air and steam, etc.). Identify the entry points to the facility—gates, turnstiles, access control portals, and doors—which should be evaluated as pathways in order to focus the analysis on the need for perimeter security and access control.

— Column 1 is for the team to list relevant assets. Similar assets within a facility with similar geographic locations on the property, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set.

— Column 2 is the type of asset (pathway, asset, activity).

— Column 3 is to document the function of the asset, pathway, or activity.

— Column 4 is to document the infrastructure/dependence and interdependence of the asset.

— Columns 5a, 5b, 5c, 5d, and 5e are for rating (VL-L-M-H-VH) the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen (this is a maximum expected damage screening assessment for casualties, environment, replacement cost, business interruption, and damage to reputation).

— Column 6 may be used to summarize ratings from Column 5a through Column 5d and to further document any asset-specific consequence information.

— Column 7 ranks the estimated overall severity of the loss of the asset, using a five-level severity ranking scale for consequences to determine the initial severity of a consequence without consideration of any existing countermeasures (C).

Form 1—Characterization

Analyze Assets and Criticality; Determine Target Assets

Date:

Facility/Operation:

Reference:

Assets	Asset Type	Function	Infrastructure Interdependence	Casualties	Environment	Replacement	Business	Reputation	Consequence	Asset Severity Ranking

A.2 Form 2—Threat Assessment Form

Document the threats against the facility.

— Column 1 shows the general types of threats that will be considered (possibly terrorists, disgruntled employees or contractors, criminals, or activists, but more specific or other groups can be considered as required for each facility-specific threat assessment).

— Column 2 is the threat category [EXT—external (outsider), INT—internal (insider), COL—collusion (between external and internal adversaries)].

— Column 3 documents the general threat of that type against this or similar assets regionally, nationally, or worldwide.

— Column 4 documents the site-specific threat history for the facility being evaluated.

— Column 5 documents the potential actions that the threat could take.

— Column 6 documents and ranks the level of capability of the threat from insignificant to critical (I-L-M-H-C).

— Column 7 documents the threat's level of motivation and intent.

— Column 8 provides an overall threat ranking assessment.

— Column 9 provides the numeric rating per the five-point threat ranking scale.

Form 2—Threat Assessment
Analyze Critical Threats

Threat	Category	General Threat History	Site-specific Threat History	Potential Actions	Threat Capability	Threat Motivation/Intent	Overall Assessment	Threat Ranking

A.3 Form 3—Attractiveness Form

— Column 1 (assets) and Column 3 (asset severity ranking) are repeated from Form 1 for reference.

— Column 2 is a documented rationale for why the particular asset is attractive (or unattractive) to each applicable threat.

— Columns 2a1, 2b1, 2c1, 2d1, etc. reflect the rationale for the ranking, and Columns 2a2, 2b2, 2c2, 2d2, etc. are the rankings of that related attractiveness on a five-point relative attractiveness ranking scale. This is repeated for each of the other credible threats.

— Column 4 is an overall target ranking (TR) per the five-point scale and is considered to be the highest attractiveness of any of the individual threat rankings but also considers that the sum of the different threats' interests may make the asset even more attractive. The TR is used to judge the degree of attractiveness of the target considering all the threats. It is used to identify the assets with the highest aggregate unconditional threat profile.

Form 3—Attractiveness Assessment

Determine Target Attractiveness Against a Specific Threat

Assets	Asset Attractiveness														Asset Severity Ranking	Target Ranking
	Threats															
	Threat 1		Threat 2		Threat 3		Threat 4		Threat 5		Threat 6		Threat 7			
	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*		

A.4 Form 4—Vulnerability Analysis and Risk Assessment Form

— Column 1 is the security event type (common security events including unauthorized access, loss of containment, degradation of the asset, theft, contamination, disruption of operations, etc.).

— Column 2 is the threat category (threat type such as terrorist, disgruntled individual, criminal, or activist).

— Column 3 is the type of threat (insider/external/collusion).

— Column 4 describes the scenario that the identified threat perpetrates to attack the identified critical asset.

— Column 5 describes the consequences of destruction, loss, or theft of the asset.

— Column 6 captures the existing safeguards/countermeasures, which consider the strategies to deter, detect, delay, respond, and recover.

— Column 7 captures the vulnerability of the critical asset to the postulated scenario, taking into account the existing countermeasures (Column 6).

— Column 8 is the ranking of vulnerability (Column 7) as likelihood of attack success (L_2 = V), using the likelihood scale 1 to 5.

— Column 9 is the **scenario-specific consequence** (based on the initial consequence from Column 5), using the severity scale 1 to 5.

— Column 10 is the threat (T) number imported from the threat worksheet, using the threat scale 1 to 5.

— Column 11 is the attractiveness (A) number imported from the attractiveness worksheet, using the attractiveness scale 1 to 5 captured as a decimal value 0.0 to 1.0.

— Column 12 is the calculation for overall likelihood, which includes $L_1 \times L_2$ [$T \times A$ (Column 10 $\times$ Column 11)] times vulnerability (V).

— Column 13 is the mitigated risk (R_1) to the asset, derived from plotting L_1 (Column 12) times V (L_2—in Column 8) on the likelihood axis and C_1 (Column 10) on the consequence severity axis of the SRA risk matrix to yield a color and a corresponding 1 to 5 risk number.

— If additional measures are needed to reduce the risk to a more acceptable level, Column 14 captures the recommended scenario-specific security upgrades and countermeasures proposed by the team.

Form 4—Vulnerability Assessment and Risk Evaluation

Conduct Scenario Analysis and Assess Risk Against Security Criteria

Security Event Type	Threat	Threat Type	Scenario	Consequences	Existing Countermeasures	Vulnerability	V	T	A	$L = L_1 \times L_2$	C_1	R_1	Proposed Countermeasures

A.5 Form 5—Recommendation Form

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 documents all the places in the SRA where that specific recommendation is identified as necessary to reduce risk.

— Column 7 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 8 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of recommendations.

— Column 9 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 7) and V_2 (Column 8).

— Column 10 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 11 captures additional comments.

Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Applicable Scenarios	Residual Risk			Priority	Comments
	C_1	$L_1 \times L_2$	R_1			C_2	V_2	R_2		

A.6 Alternate Form 5—Determine Residual Risk Based on Implementation of All Proposed Countermeasures

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 7 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 8 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 6) and V_2 (Column 7).

— Column 9 captures additional comments.

Alternate Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Residual Risk			Comments
	C_1	$L_1 \times L_2$	R_1		C_2	V_2	R_2	

A.7 Optional Form 6 (if Alternate Form 5 is Used)—Proposed Countermeasure Risk Score and Priority Form

— Column 1 identifies each unique proposed additional security upgrade or countermeasure.

— Column 2 provides the reference number for each scenario within the SRA where the countermeasure in Column 1 is recommended.

— Columns 3a, 3b, 3c, 3d, and 3e capture the initial risk (R_1) across a scenarios before the recommendation was implemented.

— Column 4 presents a mathematical total of all R_1 exposures where the recommendation was to be applied to reduce risk.

— Columns 5a, 5b, 5c, 5d, and 5e capture the residual risk (R_2) across all scenarios after the recommendation was implemented.

— Column 6 presents a mathematical total of all R_2 residual exposures where the recommendation was implemented to reduce risk.

— Column 7 reflects the expected overall "risk reduction" from R_1 to R_2 if the proposed recommendation is implemented.

— Column 8 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 9 captures additional comments.

Optional Form 6: Proposed Countermeasure Risk Reduction Score and Priority

Proposed Countermeasures	Applicable Scenarios—Reference Numbers	R_1 Risk Score	VH	H	M	L	VL	R_2 Risk Score	Risk Reduction	Overall Priority	Comments

Annex B
(informative)

SRA Supporting Data Requirements

API SRA Methodology Supporting Data	
Category [a]	**Description**
A	Scaled drawings of the overall facility and the surrounding community (e.g. plot plan of facility, area map of community up to worst case scenario radius minimum).
A	Aerial photography of the facility and surrounding community (if available).
A	Information such as general process description, process flow diagrams, or block flow diagrams that describes basic operations of the process including raw materials, feedstocks, intermediates, products, utilities, and waste streams.
A	Information (e.g. drawings that identify physical locations and routing) that describes the infrastructures upon which the facility relies [e.g. electric power, natural gas, petroleum fuels, telecommunications, transportation (road, rail, water, air), water/wastewater].
A	Historical security incident information.
A	Description of guard force, physical security measures, electronic security measures, security policies.
A	Threat information specific to the company (if available).
A	Historical security assessment information and threat data
B	Specifications and descriptions for security related equipment and systems. Plot plan showing existing security countermeasures.
B	Other related information including chemical or process registrations and off-site consequence analysis (if applicable, or similar information).
B	Most up-to-date process hazard analysis reports for processes areas.
B	Emergency response plans and procedures (site, community response, and corporate contingency plans) and crisis management plans and procedures (site and corporate).
B	Information on hazardous materials' physical and hazard properties
B	Complete a SRA chemicals checklist to determine whether the site handles any hazardous materials on referenced regulatory applicability lists such as:
C	— EPA risk management program standard 40 *CFR* Part 68;
C	— OSHA process safety management standard 29 *CFR* 1910.119;
C	— Chemical Weapons Convention, Schedule 2 and specifically listed Schedule 3 chemicals;
C	— the Australia Group list of chemical and biological weapons.
C	Design basis for the processes (as required).
C	Unit plot plans of the processes.
C	Process flow diagrams and piping and instrument diagrams for process streams with hazardous materials.
C	Safety systems including fire protection, detection, spill suppression systems.
C	Information regarding the safety instrumented systems (SIS), programmable logic controllers, process control systems.
C	Operating procedures for start-up, shutdown, and emergency (operators may provide general overview of this information, with written information available as required).
C	Mechanical equipment drawings for critical equipment containing hazardous chemicals.
C	Electrical one-line diagrams.
C	Control system logic diagrams.
C	Equipment data information.
C	Information on materials of construction and their properties.
C	Information on critical utilities used in the process.
C	Test and maintenance procedures for security related equipment and systems.

[a] Categories:

A = Documentation to be provided to SRA team as much in advance as possible before arrival for familiarization.

B = Documentation to be gathered for use in SRA team meetings on site.

C = Documentation that should be readily available on an as-needed basis.

Annex C
(informative)

Examples of the SRA Process

C.1 Introduction

The general approach is to apply risk assessment resources and, ultimately, special security resources, primarily where justified based on the SRA results. The SRA process involves consideration of facilities from both the general viewpoint and the specific asset viewpoint. Consideration at the general level is useful for determination of overall impacts of loss, infrastructure, and interdependencies at the system level, which is represented in the methodology by "C_1," the mitigated consequences, and R_1, the mitigated risk. 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, which is represented in the methodology by C_2, scenario-specific consequences, and R_2, the residual risk.

It is presumed that all facilities will maintain a minimum level of security with general countermeasures such as access controls, shutdown strategies, and response to security incidents. Certain assets will justify a more specific level of security based on their value and expected level of interest to threats. That interest is represented in the methodology by the factors of threat (T) and attractiveness (A).

Likelihood is a function of the chance of being targeted for an act and the conditional chance of a successful act (i.e. both planning and execution) given the threat (which considers the threat's actions and choices) and given the options available against existing security measures. The combination of the two factors threat (T) and attractiveness (A) produce a surrogate estimate for the likelihood of the act (L_1) for each scenario, which is either a probability of the event or a frequency over a given period of time such as the life of the operation. Vulnerability (V) is a surrogate for the likelihood of expected success (L_2) for each scenario (L_2 = V), which can be expressed as a numeric value ranging from 1 to 5 that corresponds to a conditional probability that the threat will succeed if the event occurs.

The API SRA 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 SRA team gaining an understanding of the facility and the surrounding neighborhood, the assets that comprise the facility including their functions and interdependencies, as well as the associated hazards and consequences if these assets or functions are compromised. This is accomplished in Step 1: Asset Characterization, by completing Form 1—Characterization, and results in an understanding of which assets and functions are "critical" to operations. Criticality may be defined both in terms of the potential impact to the workers, community, the environment, and the company, as well as to the business importance and continuity of the system. For example, a large gasoline storage tank may be a critical part of the operation because of the inability to operate without the availability of that tank to hold and dispense refined products or the potential that an attack on the tank would likely yield significant consequences. As such it may be given a high priority for further analysis and special security countermeasures.

Based on this first level of screening (i.e. analyzing all assets in order to determine the critical assets), a critical asset list is produced. Next, the critical assets are reviewed in light of the threats. Threats may have different objectives, so the critical asset list is reviewed from each threat's perspective and an asset attractiveness ranking (A) is given. This factor is a quick measure of whether the threat would value damaging, compromising, or stealing the asset (or the material contained within the asset), which serves as an indicator of the likelihood that a given threat 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 SRA. A target may optionally receive further specific analysis, including the development of scenarios to determine and test perceived vulnerabilities. All assets receive a general security review and a baseline security survey prior to determination if additional analysis will be required.

Regardless of the type of facility, the study is conducted in a top-down, systematic manner, and the five steps of the process are documented using worksheet forms, following the logic flowchart for the SRA as shown in Figure C.1.

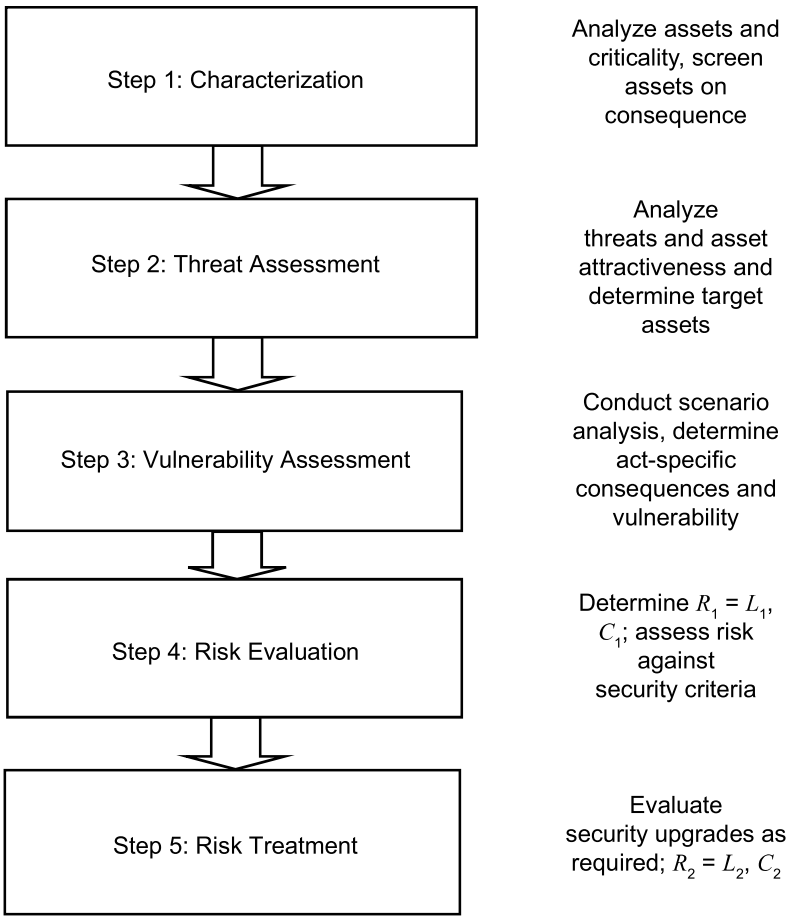

Figure C.1—API SRA Methodology Flow Diagram

C.2 Examples

C.2.1 General

This annex provides five examples of how the SRA could be documented by using the appropriate forms for the following types of facilities.

— Example 1: Petroleum Distribution Terminal.

— Example 2: Refinery.

— Example 3: Pipeline.

— Example 4: Truck Transportation.

— Example 5: Rail Transportation.

C.2.2 Example 1: Petroleum Distribution Terminal

C.2.2.1 General

The application of the API SRA methodology to a typical petroleum distribution terminal is illustrated in the following example and in Figure C.2. Only the first page or two of each of the forms is shown for illustrative purposes. It is assumed that the study is conducted by the owner/operator of the terminal, and the various interfaces with customers and suppliers are evaluated, but the responsibility for security of the terminal itself rests with the owners/operators.

C.2.2.2 Form 1—Characterization Form

All entry points to the facility—gates, turnstiles, access control portals, and doors—should be evaluated as pathways in order to focus the analysis on the need for perimeter security and access control. Determine the major assets of the facility including process units, control rooms, tankage, truck and rail bays, marine loading or unloading points, communications networks, pipeline manifolds, utilities, and supporting infrastructure (e.g. motor control centers, vapor recovery units, raw water intake, electrical power, process air and steam, etc.).

— Column 1 is for the team to list all relevant assets. Similar assets within a facility with similar geographic locations on the property, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set.

— Column 2 is the type of asset (pathway, asset, activity).

— Column 3 is to document the function of the asset, pathway, or activity.

— Column 4 is to document the infrastructure/dependence and interdependence of the asset.

— Columns 5a, 5b, 5c, 5d, and 5e are for rating (VL-L-M-H-VH) the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen (this is a maximum expected damage screening assessment for casualties, environment, replacement cost, business interruption, and damage to reputation).

— Column 6 may be used to summarize ratings from Column 5a through Column 5d and to further document any asset-specific consequence information.

— Column 7 ranks the estimated overall severity of the loss of the asset, using a five-level severity ranking scale for consequence to determine the initial severity of consequence without consideration of any existing countermeasures (C).

C.2.2.3 Form 2—Threat Assessment

Document the threats against the facility.

— Column 1 shows the general types of threats that will be considered (possibly terrorists, disgruntled employees or contractors, criminals, or activists, but more specific or other groups can be considered as required for each facility-specific threat assessment).

— Column 2 is threat category [EXT—external (outsider), INT—internal (insider), COL—collusion (between external and internal adversaries)].

— Column 3 documents the general threat of that type against this or similar assets regionally, nationally, or worldwide.

— Column 4 documents the site-specific threat history for the facility being evaluated.

— Column 5 documents the potential actions that the threat could take.

— Column 6 documents and ranks the level of capability of the threat from insignificant to critical (I-L-M-H-C).

— Column 7 documents the threat's level of motivation and intent.

— Column 8 provides an overall threat ranking assessment.

— Column 9 provides the numeric rating per the five-point threat ranking scale.

C.2.2.4 Form 3—Attractiveness Assessment

— Column 1 (assets) and Column 3 (asset severity ranking) are repeated from Form 1 for reference.

— Column 2 is a documented rationale for why the particular asset is attractive (or unattractive) to each applicable threat.

— Columns 2a1, 2b1, 2c1, 2d1, etc. reflect the rationale for the ranking, and Columns 2a2, 2b2, 2c2, 2d2, etc. are the ranking of that related attractiveness on a five-point relative attractiveness ranking scale. This is repeated for each of the other credible threats.

— Column 4 is an overall TR per the five-point scale and is considered to be the highest attractiveness of any of the individual threat rankings but also considers that the sum of the different threats' interests may make the asset even more attractive. The target ranking is used to judge the degree of attractiveness of the target considering all the threats. It is used to identify the assets with the highest aggregate unconditional threat profile.

C.2.2.5 Form 4—Vulnerability Assessment and Risk Evaluation

— Column 1 is the security event type (common security events including unauthorized access, loss of containment, degradation of the asset, theft, contamination, disruption of operations, etc.).

— Column 2 is the threat category (threat type such as terrorist, disgruntled individual, criminal, or activist).

— Column 3 is the type of threat (insider/external/collusion).

— Column 4 describes the malevolent scenario that the identified threat perpetrates to attack the identified critical asset.

— Column 5 describes the consequences of destruction, loss, or theft of the asset.

— Column 6 captures the existing safeguards/countermeasures, which consider the strategies to deter, detect, delay, and respond.

— Column 7 captures the vulnerability of the critical asset to the postulated scenario, taking into account the existing countermeasures (Column 6).

— Column 8 is the ranking of vulnerability (Column 7) as likelihood of attack success (L_2 = V), using the likelihood scale from 1 to 5.

— Column 9 is the scenario-specific consequence (from Column 5), using the severity scale 1 to 5.

— Column 10 is the threat (T) number imported from the threat worksheet, using the threat scale 1 to 5.

— Column 11 is the attractiveness (A) number imported from attractiveness worksheet, using the attractiveness scale 1 to 5 captured as a decimal value 0.0 to 1.0.

— Column 12 is the calculation for overall likelihood, which includes $L_1 \times L_2$ [$T \times A$ (Column 10 x Column 11)] times vulnerability (V).

— Column 13 is the mitigated risk (R_1) to the asset, derived from plotting L_1 (Column 12) times V (L_2—in Column 8) on the likelihood axis and C_1 (Column 10) on the consequence severity axis of the SRA risk matrix to yield a color and a corresponding 1 to 5 risk number.

— If additional measures are needed to reduce the risk to a more acceptable level, Column 14 captures the recommended scenario-specific security upgrades and countermeasures proposed by the team.

C.2.2.6 Form 5—Proposed Recommendations and Residual Risk

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 documents all the places in the SRA where that specific recommendation is identified as necessary to reduce risk.

— Column 7 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 8 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 9 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 7) and V_2 (Column 8).

— Column 10 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 11 captures any additional comments.

C.2.2.7 Alternate Form 5—Determine Residual Risk Based on Implementation of All Proposed Countermeasures

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 7 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 8 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 6) and V_2 (Column 7).

— Column 9 captures any additional comments.

C.2.2.8 Optional Form 6 (if Alternate Form 5 is Used)—Proposed Countermeasure Risk Score and Priority Form

— Column 1 identifies each unique proposed additional security upgrade or countermeasure.

— Column 2 provides the reference number for each scenario within the SRA where the countermeasure in Column 1 is recommended.

— Columns 3a, 3b, 3c, 3d, and 3e capture the initial risk (R_1) across a scenarios before the recommendation was implemented.

— Column 4 presents a mathematical total of all R_1 exposures where the recommendation was to be applied to reduce risk.

— Columns 5a, 5b, 5c, 5d, and 5e capture the residual risk (R_2) across all scenarios after the recommendation was implemented.

— Column 6 presents a mathematical total of all R_2 residual exposures where the recommendation was implemented to reduce risk.

— Column 7 reflects the expected overall “risk reduction” from R_1 to R_2 if the proposed recommendation is implemented

— Column 8 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 9 captures any additional comments.

C.2.2.9 Responsibilities

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

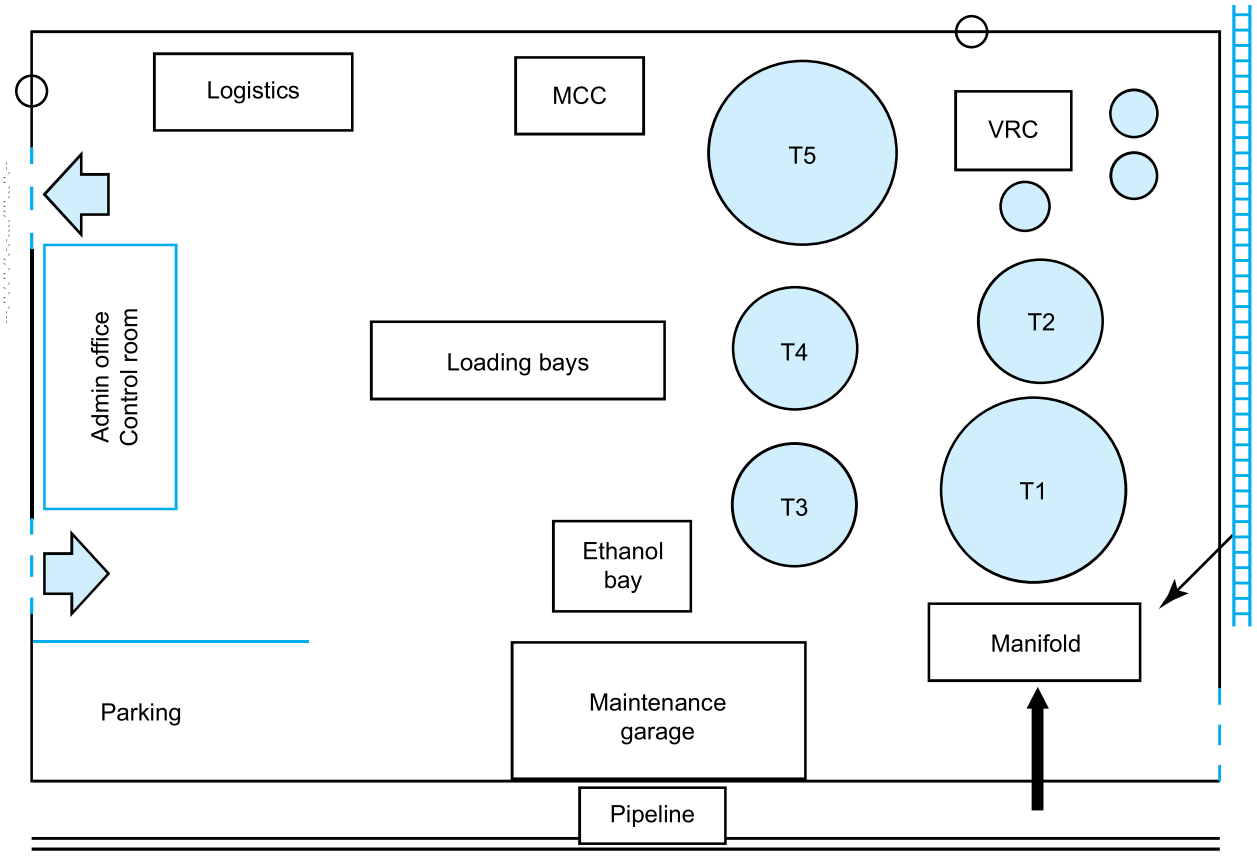

Figure C.2—Example Terminal Diagram

Date: Facility/Operation: Reference:	Form 1—Characterization Analyze Assets and Criticality; Determine Target Assets									
Assets	**Asset Type**	**Function**	**Infrastructure Interdependence**	**Casualties**	**Environment**	**Replacement**	**Business**	**Reputation**	**Consequence**	**Asset Severity Ranking**
1. Main Entrance Gate 1.	Pathway	Single horizontal sliding chain linked fence gate on wheels; electrically driven with chain drive; access control system via key, remote control, or loading card (no PIN required) on ingress; egress is magnetic ground loop; main gate is operable through access card system and manual button. Equipped with CCTV monitored in the SOC. Not crash rated.	Dependent on the main gate for all vehicle entrance; disruption of entrance gate is significant, but terminal could still operate in limited capacity by using exit gate for in/out traffic; gate is a possible pathway for illegal entry.	3	4	3	4	2	Team believes that this pathway should be included in the assessment. It provides potential access to site facilities, chemicals of interest, and sensitive information.	4
2. Emergency Exit Only pedestrian turnstiles (2).	Pathway	Single high throughout “exit-only” rotating gate for terminal evacuation in emergency situations. Equipped with CCTV monitored at SOC.	Crash-rated barrier, no access from outside the terminal. Pedestrian exit only with barriers and direction flow to prevent unauthorized access.	1	1	1	1	1	Team does not believe that this pathway should be included for further analysis. It does not provide access to the site assets.	2
7. Tanks T1, T2 (gasoline).	Asset	2 aboveground storage tanks: T1 plus T2 = 50,000 bbl gasoline-flammable material in same diked area.	The entire operation would be inoperative until repaired.	3	4	3	4	2	Potential off-site public exposure; business interruption; possible personnel hazard; possible environmental release. To rebuild any one tank >$1 MM less than $10 MM.	4

Form 2—Threat Assessment

Analyze Critical Threats

Threat	Category	General Threat History	Site-specific Threat History	Potential Actions	Threat Capability	Threat Motivation/Intent	Overall Assessment	Threat Ranking
1. Terrorists	I/E/C	General terrorist activity including 9/11/2001 attacks and subsequent disruption of cells in North America with stated goals targeting oil, gas, refining, and chemicals.	The facility has not experienced any specific terrorist activities directed against the facility or towards other similar facilities in the area.	Explosive destruction of critical refining assets, targeted against facilities. Use of stealth or force to cause release of hydrocarbons or toxic chemicals; possible theft of hydrocarbons; possible contamination.	Can easily overwhelm company security, good organizational support, resources, financial backing, network of members, highly developed communication capabilities highly capable, sufficient resources for attack highly trained, access to small or large arms.	Assume this adversary is highly motivated, likely extremist, prepared to die for their cause, and intent to cause maximum harm to company assets including loss of life and economic disruption.	Medium	3
2. Disgruntled employee/ contractor.	I/E	Sabotage, work stoppages, workplace violence; theft of equipment, information; destruction of information or equipment.	The facility has not experienced any specific disgruntled employee or contractor activities directed against company assets, but nearby terminals have experienced security events related to disgruntled personnel sabotage.	Sabotage to equipment causing possible release of hazardous materials, contamination of products, environmental impact, or major equipment damage and business interruption. Possible for nuisance threats, particularly from contract workers with intent to disrupt operations.	Insider access, knowledge, and able to independently operate with authorization and without question; may have access to physical keys, computer passwords, gate access codes, communication equipment, records, business confidential information; vehicles, proximity cards for access cards, access to process control system.	Nuisance adversary is intent to cause inconvenience and financial impacts to the company or their employer. If very disgruntled or troubled, intent and motivation could be extreme to cause maximum damage, possibly with personal sacrifice as evidenced in various national workplace violence cases.	Medium	3
3. Criminal	I/E	Criminal activities including theft of critical equipment or proprietary information for personal gain.	The facility has not experienced any specific criminal activities but other terminals have had tanker trucks stolen.	Criminal activities including theft of critical equipment or proprietary information for personal gain.	Willing to engage in a variety of illegal acts, willing to take advantage of opportunities to remove or divert company assets, equipment, information, or refined products.	Highly motivated criminals; possible presence of organized crime.	Medium	3

Form 3—Attractiveness Assessment

Determine Target Attractiveness Against a Specific Threat

Assets	Asset Attractiveness														Asset Severity Ranking	Target Ranking
	Threats															
	Threat 1		Threat 2		Threat 3		Threat 4		Threat 5		Threat 6		Threat 7			
	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*		
1. Main Entrance Gate 1.	One of most likely pathways for a vehicle borne improvised explosive device (VBIED) to gain access to the terminal.	3	Normal point of access for current employees and contractors.	3	Most likely point of attempted breach.	3									3	2
2. Emergency Exit Only pedestrian turnstiles.															1	1
7. Tanks T1, T2 (gasoline).	Potential for large flammable liquids fire and for effecting the terminal generally; possible for major disruption to operations and for collateral damage to entire tank farm.	4	The disgruntled current or former employee or contractor could be interested in this asset.	3	Unlikely theft interest.	2									4	4

Form 4—Vulnerability Assessment and Risk Evaluation

Conduct Scenario Analysis and Assess Risk Against Security Criteria

Security Event Type	Threat	Threat Type	Scenario	Consequences	Existing Countermeasures	Vulnerability	V	T	A	$L = L_1 \times L_2$	C_1	R_1	Proposed Countermeasures
Unauthorized access.	Terrorist	I/E/C	Terrorist in VBIED defeats main gate to access the terminal.	Unauthorized access to chemicals.	1.1. Normally closed electrically operated gate. 1.2. Magnetic stripe and remote operable and key access control system for the gate. 1.3. Camera only on the exit gate. 1.4. Response by local law enforcement. 1.5. Operators or drivers may be in the area. 1.6. Security awareness and vigilance training. 1.7. Lighting.	1.1.1. Gate is not resistant to vehicle attack. 1.1.2. Gate has a long delay for closure allowing piggy backing. 1.1.3. Gate is not equipped with intrusion detection for unauthorized access. 1.1.4 Police arrival at the gate may take 5 minutes. 1.1.5. Limited surveillance.	4	3	0.8	3	3	3	1. Increase crash resistivity of the main gate to K12. 2. Adjust the main gate closure delay to prevent piggybacking. 3. Place a STOP sign inside the main gate for truckers to stop and wait for the gate to close before proceeding. 4. Install intrusion detection sensors on perimeter fencing and gates. 5. Install CCTV on critical assets. 6. Coordinate with local law enforcement to improve response time.

Form 4—Vulnerability Assessment and Risk Evaluation (Continued)

Conduct Scenario Analysis and Assess Risk Against Security Criteria

Security Event Type	Threat	Threat Type	Scenario	Consequences	Existing Countermeasures	Vulnerability	V	T	A	$L = L_1 \times L_2$	C_1	R_1	Proposed Countermeasures
Loss of containment.	Terrorist	I/E/C	Terrorist with VBIED uses explosive attack against the T1-T2 gasoline tanks.	Potential fire and explosion with injuries on site and possible exposure to the public. Environmental release. Loss of company assets. Loss of company reputation. Severe business interruption. Exposure to negative publicity. Exposure to litigation. Loss of product and economic impacts.	Armed response by local law enforcement. Each operator is equipped with a radio for communication. Lighting. Operations personnel may be in the area.	1.1.1. Limited surveillance. 1.1.2. Police arrival at the gate may take 5 minutes. 1.1.4. Security response is not integrated. 1.1.3. Security forces do not conduct patrol rounds.	4	3	1.0	4	4	4	5. Install CCTV on critical assets. 6. Coordinate with local law enforcement to improve response time. 7. Conduct drills and exercises with local law enforcement and site security to improve integrated response. 8. Modify security post orders to require patrol rounds on a frequent but unscheduled basis.

Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Applicable Scenarios	Residual Risk			Priority	Comments
	C_1	$L_1 \times L_2$	R_1			C_2	V_2	R_2		
Terrorist in VBIED defeats main gate to access the terminal.	3	3	3	1. Increase crash resistivity of the main gate to K12. 2. Adjust the main gate closure delay to prevent piggybacking. 3. Place a STOP sign inside the main gate for truckers to stop and wait for the gate to close before proceeding. 4. Install intrusion detection sensors on perimeter fencing and gates. 5. Install CCTV on critical assets. 6. Coordinate with local law enforcement to improve response time.	1.1	3	2	2	1	Because of cost considerations, the installation of CCTV may need to be delayed until the next budget cycle.
Terrorist in VBIED defeats main gate to access the terminal.	3	4	4	5. Install CCTV on critical assets. 6. Coordinate with local law enforcement to improve response time. 7. Conduct drills and exercises with local law enforcement and site security to improve integrated response. 8. Modify security post orders to require patrol rounds on a frequent but unscheduled basis.	1.2	3	3	3	2	Because of cost considerations, the installation of CCTV may need to be delayed until the next budget cycle.

Alternate Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Residual Risk			Comments
	C_1	$L_1 \times L_2$	R_1		C_2	V_2	R_2	
Terrorist in VBIED defeats main gate to access the terminal.	3	3	3	1. Increase crash resistivity of the main gate to K12. 2. Adjust the main gate closure delay to prevent piggybacking. 3. Place a STOP sign inside the main gate for truckers to stop and wait for the gate to close before proceeding. 4. Install intrusion detection sensors on perimeter fencing and gates. 5. Install CCTV on critical assets. 6. Coordinate with local law enforcement to improve response time.	3	2	2	Because of cost considerations, the installation of CCTV may need to be delayed until the next budget cycle.
Terrorist in VBIED defeats main gate to access the terminal.	3	4	4	5. Install CCTV on critical assets. 6. Coordinate with local law enforcement to improve response time. 7. Conduct drills and exercises with local law enforcement and site security to improve integrated response. 8. Modify security post orders to require patrol rounds on a frequent but unscheduled basis.	3	3	3	Because of cost considerations, the installation of CCTV may need to be delayed until the next budget cycle.

Optional Form 6: Proposed Countermeasure Risk Reduction Score and Priority

Proposed Countermeasures	Applicable Scenarios—Reference Numbers	VH	H	M	L	VL	R_1 Risk Score	VH	H	M	L	VL	R_2 Risk Score	Risk Reduction	Overall Priority	Comments
6. Coordinate with local law enforcement to improve response time.	1.2; 1.2		4	3			7			3	2		5	2	1	
5. Install CCTV on critical assets.	1.1; 1.2		4	3			7			3	2		5	2	2	
1. Increase crash resistivity of the main gate to K12.	1.1			3			3				2		2	1	3	
2. Adjust the main gate closure delay to prevent piggybacking.	1.1			3			3				2		2	1	4	
8. Modify security post orders to require patrol rounds on a frequent but unscheduled basis.	1.2		4				4			3			3	1	5	
3. Place a STOP sign inside the main gate for truckers to stop and wait for the gate to close before proceeding.	1.1			3			3				2		2	1	6	
7. Conduct drills and exercises with local law enforcement and site security to improve integrated response.	1.2		4				4			3			3	1	7	
4. Install intrusion detection sensors on perimeter fencing and gates.	1.1			3			3				2		2	1	8	

C.2.3 Example 2: Refinery

C.2.3.1 General

The application of the API SRA methodology to a typical refinery is illustrated in the following example and in Figure C.3. Only the first page of each of the forms is shown for illustrative purposes. A complete analysis will require additional forms. It is assumed that the study is conducted by the refiner and the various interfaces with customers and suppliers are evaluated, but the responsibility for security of those facilities rests with the owners.

C.2.3.2 Form 1—Characterization Form

All entry points to the facility—gates, turnstiles, access control portals, and doors—should be evaluated as pathways in order to focus the analysis on the need for perimeter security and access control. Determine the major assets of the facility including process units, control rooms, tankage, truck and rail bays, marine loading or unloading points, communications networks, pipeline manifolds, utilities, and supporting infrastructure (e.g. motor control centers, vapor recovery units, raw water intake, electrical power, process air and steam, etc.).

— Column 1 is for the team to list all relevant assets. Similar assets within a facility with similar geographic locations on the property, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set;

— Column 2 is the type of asset (pathway, asset, activity)

— Column 3 is to document the function of the asset, pathway, or activity;

— Column 4 is to document the Infrastructure/dependence and Interdependence of the asset;

— Columns 5a, 5b, 5c, 5d, and 5e are for rating (VL-L-M-H-VH) the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen (this is a maximum expected damage screening assessment for casualties, environment, replacement cost, business interruption, and damage to reputation).

— Column 6 may be used to summarize ratings from Column 5a through Column 5d and to further document any asset-specific consequence information.

— Column 7 ranks the estimated overall severity of the loss of the asset, using a five-level severity ranking scale for consequence to determine the initial severity of consequence without consideration of any existing countermeasures (C).

C.2.3.3 Form 2—Threat Assessment

Document the threats against the facility.

— Column 1 shows the general types of threats that will be considered (possibly terrorists, disgruntled employees or contractors, criminals, or activists; but more specific or other groups can be considered as required for each facility-specific threat assessment).

— Column 2 is threat category [EXT—external (outsider), INT—internal (insider), COL—collusion (between external and internal adversaries)].

— Column 3 documents the general threat of that type against this or similar assets regionally, nationally, or worldwide.

— Column 4 documents the site-specific threat history for the facility being evaluated.

— Column 5 documents the potential actions that the threat could take.

— Column 6 documents and ranks the level of capability of the threat from insignificant to critical (I-L-M-H-C).

— Column 7 documents the threat's level of motivation and intent.

— Column 8 provides an overall threat ranking assessment.

— Column 9 provides the numeric rating per the five-point threat ranking scale.

C.2.3.4 Form 3—Attractiveness Assessment

— Column 1 (assets) and Column 3 (asset severity ranking) are repeated from Form 1 for reference.

— Column 2 is a documented rationale for why the particular asset is attractive (or unattractive) to each applicable threat.

— Columns 2a1, 2b1, 2c1, 2d1, etc. reflect the rationale for the ranking, and Columns 2a2, 2b2, 2c2, 2d2, etc. are the ranking of that related attractiveness on a five-point relative attractiveness ranking scale. This is repeated for each of the other credible threats.

— Column 4 is an overall TR per the five-point scale and is considered to be the highest attractiveness of any of the individual threat rankings but also considers that the sum of the different threats' interests may make the asset even more attractive. The TR is used to judge the degree of attractiveness of the target considering all the threats. It is used to identify the assets with the highest aggregate unconditional threat profile.

C.2.3.5 Form 4—Vulnerability Assessment and Risk Evaluation

— Column 1 is the security event type (common security events including unauthorized access, loss of containment, degradation of the asset, theft, contamination, disruption of operations, etc.).

— Column 2 is the threat category (threat type such as terrorist, disgruntled individual, criminal, or activist).

— Column 3 is the type of threat (insider/external/collusion).

— Column 4 describes the malevolent scenario that the identified threat perpetrates to attack the identified critical asset.

— Column 5 describes the consequences of destruction, loss, or theft of the asset.

— Column 6 captures the existing safeguards/countermeasures, which consider the strategies to deter, detect, delay, and respond.

— Column 7 captures the vulnerability of the critical asset to the postulated scenario taking into account the existing countermeasures (Column 6).

— Column 8 is the ranking of vulnerability (Column 7) as likelihood of attack success ($L_2 = V$), using the likelihood scale 1 to 5.

— Column 9 is the scenario-specific consequence (from Column 5), using the severity scale 1 to 5.

— Column 10 is the threat (T) number imported from the threat worksheet, using the threat scale 1 to 5.

— Column 11 is the attractiveness (A) number imported from attractiveness worksheet, using the attractiveness scale 1 to 5 captured as a decimal value 0.0 to 1.0.

— Column 12 is the calculation for overall likelihood, which includes $L_1 \times L_2$ [$T \times A$ (Column 10 × Column 11)] times vulnerability (V).

— Column 13 is the mitigated risk (R_1) to the asset, derived from plotting L_1 (Column 12) times V (L_2—in Column 8) on the likelihood axis and C_1 (Column 10) on the consequence severity axis of the SRA risk matrix to yield a color and a corresponding 1 to 5 risk number.

— If additional measures are needed to reduce the risk to a more acceptable level, Column 14 captures the recommended scenario-specific security upgrades and countermeasures proposed by the team.

C.2.3.6 Form 5—Proposed Recommendations and Residual Risk

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 documents all the places in the SRA where that specific recommendation is identified as necessary to reduce risk.

— Column 7 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 8 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 9 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 7) and V_2 (Column 8).

— Column 10 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 11 captures any additional comments.

C.2.3.7 Alternate Form 5—Determine Residual Risk Based on Implementation of All Proposed Countermeasures

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 7 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 8 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 6) and V_2 (Column 7).

— Column 9 captures any additional comments.

C.2.3.8 Optional Form 6 (if Alternate Form 5 is Used)—Proposed Countermeasure Risk Score and Priority Form

— Column 1 identifies each unique proposed additional security upgrade or countermeasure.

— Column 2 provides the reference number for each scenario within the SRA where the countermeasure in Column 1 is recommended.

— Columns 3a, 3b, 3c, 3d, and 3e capture the initial risk (R_1) across a scenarios before the recommendation was implemented.

— Column 4 presents a mathematical total of all R_1 exposures where the recommendation was to be applied to reduce risk.

— Columns 5a, 5b, 5c, 5d, and 5e capture the residual risk (R_2) across all scenarios after the recommendation was implemented.

— Column 6 presents a mathematical total of all R_2 residual exposures where the recommendation was implemented to reduce risk.

— Column 7 reflects the expected overall "risk reduction" from R_1 to R_2 if the proposed recommendation is implemented.

— Column 8 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 9 captures any additional comments.

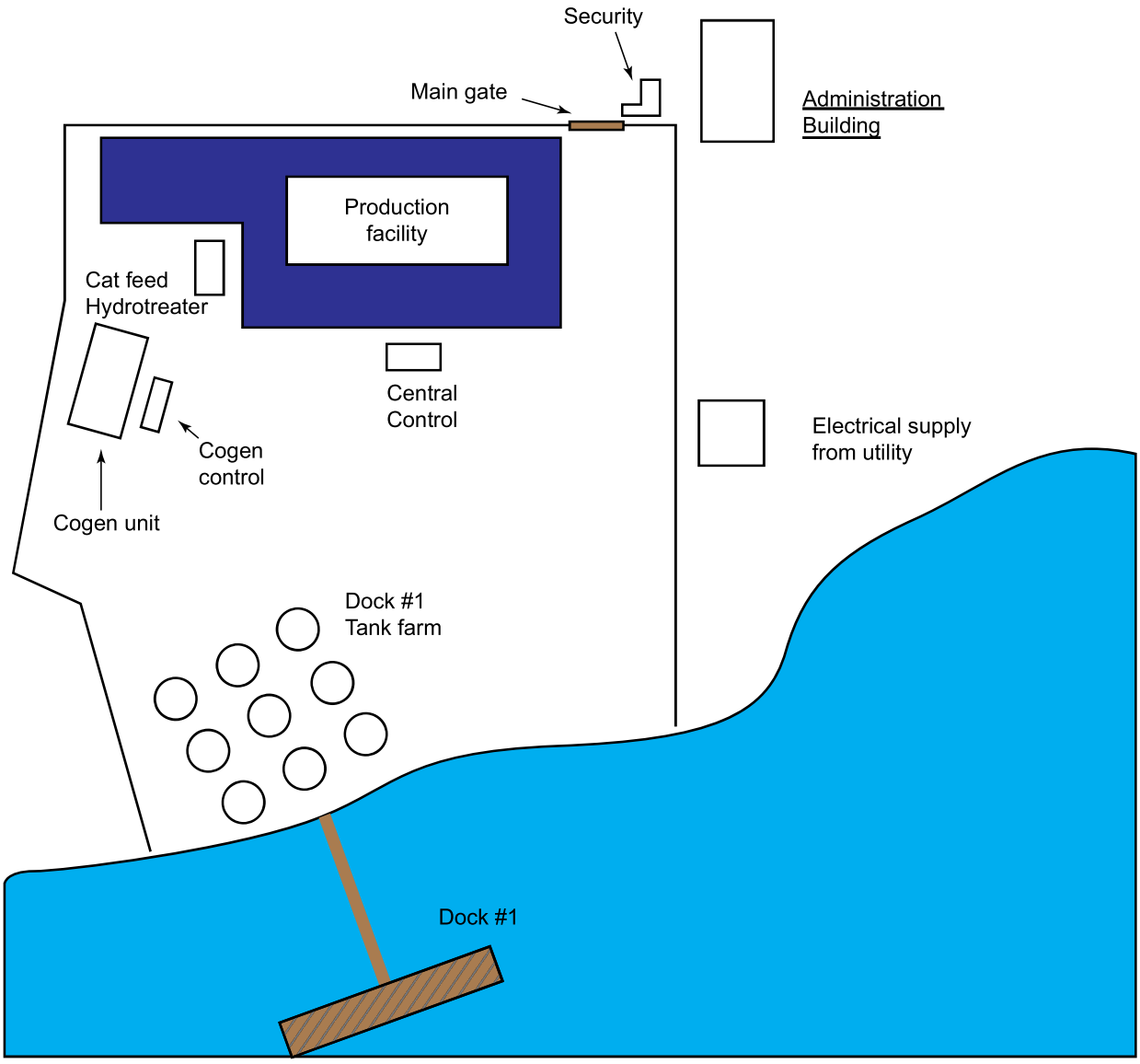

Figure C.3—Example Refinery Diagram

Date: Facility/Operation: Reference:	Form 1—Characterization Analyze Assets and Criticality; Determine Target Assets									
Assets	**Asset Type**	**Function**	**Infrastructure Interdependence**	**Casualties**	**Environment**	**Replacement**	**Business**	**Reputation**	**Consequence**	**Asset Severity Ranking**
1. Main entrance gate.	Pathway	Single horizontal sliding chain linked fence gate on wheels; electrically driven with chain drive; access control system via key, remote control, or loading card (no PIN required) on ingress; egress is magnetic ground loop; main gate is operable through access card system and manual button. Equipped with CCTV monitored in the SOC. Not crash rated.	Dependent on the main gate for all vehicle entrance; disruption of entrance gate is significant, but terminal could still operate in limited capacity by using exit gate for in/out traffic; gate is a possible pathway for illegal entry.	4	5	5	4	3	Team believes that this pathway should be included in the assessment. It provides potential access to site facilities, chemicals of interest, and sensitive information.	5
2. Central control room.	Asset	Critical security communications and monitoring; cat-cracker, Coker 1, alkylation, treating plant; and crude units.	Controls all Zone 1 processes. The distributed control systems' equipment in engineering room is critical to refinery operations. Has the Emergency Control Center and is staffed 24/7.	4	2	4	3	2	Potential for loss of life, loss of control function, and long time to repair if damaged.	4
3. Co-gen unit and control room.	Asset	Steam production and electrical power generation.	Powers all utilities (2 large transformers, 7 small transformers, and 6 diesel generators). Complete loss of the co-gen unit would cease operations because there is limited redundancy in the electrical system.	3	2	4	2	2	Alternate power supply available through Lone Star Electric within two days. Co-gen unit sells power to the grid and connections are already in place.	4
4. Dock 1.	Asset	Coker feed is critical feedstock. Coker feed, #2 fuel oil, benzene, toluene, molten sulfur in storage.	Essential waterside access for feedstock. Regulated under the Maritime Transportation Security Act.	3	5	5	4	3	Significant environmental damage and replacement cost.	5

Date: Facility/Operation: Reference:	Form 1—Characterization (Continued) Analyze Assets and Criticality; Determine Target Assets									
Assets	**Asset Type**	**Function**	**Infrastructure Interdependence**	**Casualties**	**Environment**	**Replacement**	**Business**	**Reputation**	**Consequence**	**Asset Severity Ranking**
5. Dock 1 Tank Farm—Storage in atmospheric tanks north of Dock 1 (crude inT-800; T-802; T-803,T-805; ballast/slop oil tank T-804; lube oils in T-240 to T-244).	Asset	Crude, intermediate, waste, and finished liquid hydrocarbons storage.	Refinery needs storage to operate but could run at limited capacity for approximately 10 days.	2	3	3	2	3	Pipeline dock is in restricted area and replacement should take less than a month is pipe is damaged; however, a work around a damaged section should take less than a week.	3

Form 2—Threat Assessment

Analyze Critical Threats

Threat	Category	General Threat History	Site-specific Threat History	Potential Actions	Threat Capability	Threat Motivation/Intent	Overall Assessment	Threat Ranking
1. Terrorists.	EXT	General terrorist activity including 9/11/2001 attacks and subsequent disruption of cells in North America with stated goals targeting oil, gas, refining, and chemicals.	The facility has not experienced any specific terrorist activities directed against the facility or towards other similar facilities in the area.	Use explosives or small arms to destroy target. May be interested in theft of products of value to terrorist organizations for secondary attack.	Use of improvised explosive device possibly involving a vehicle is most likely scenario. Assume trained, with good information and significant resources to plan and execute attack.	Assume highly motivated to cause maximum damage to critical infrastructure and casualties.	Medium	3
2. Disgruntled employee/ contractor.	INT	Sabotage, work stoppages, workplace violence; theft of equipment, information; destruction of information or equipment.	The facility has not experienced any specific disgruntled employee or contractor activities directed against company assets.	Might cause intentional overfill of tank or damage to equipment leading to release; might cause product contamination; possible for explosion.	Specialized insider knowledge and training. Unrestricted access to entire facility. Not likely to use weapons if sabotage but may use small arms if workplace violence.	Potential for disgruntled employee because of disciplinary action; other workplace violence reasons; possibly in collusion with outside terrorist group in extreme case.	Medium	3
3. Activist.	EXT	Disruption of operations, theft of equipment or proprietary information.	Citizens for Green Environment has repeatedly staged demonstrations and expressed interest in shutting down refinery operations.	Possibly interested in causing public embarrassment; temporary shutdown of plant; long range goal of elimination of toxic substance in use.	Highly organized and well-funded to cause staged attack of multiple facility operations simultaneously (dock, rail, gate).	Highly politically charged and motivated.	High	4

Form 3—Attractiveness Assessment

Determine Target Attractiveness Against a Specific Threat

Assets	Asset Attractiveness														Asset Severity Ranking	Target Ranking
	Threats															
	Threat 1		Threat 2		Threat 3		Threat 4		Threat 5		Threat 6		Threat 7			
	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*		
1. Main Entrance Gate 1.	One of most likely pathways for a VBIED to gain access to the refinery.	3	Normal point of access for current employees and contractors.	3	Most likely point of attempted breach and demonstration .	4									3	3
2. Central control room.	Provides access to control multiple units at the same time but does not ensure the level of consequence usually sought by this threat.	3	Maybe recognizable target; insider information on process control and access; high concentration of processes under single control and large numbers of operators in plant.	3	Not easily accessible; does not provide opportunity for media attention and requires trespassing.	2									4	3
3. Dock 1.	Immediately accessible from waterside; recognizable and understood critical.	4	Accessibility; understood; critical operation; long time for repair.	3	Easily accessible by water; provides opportunity for media attention; activist activity.	4									5	4

Form 4—Vulnerability Assessment and Risk Evaluation

Conduct Scenario Analysis and Assess Risk Against Security Criteria

Security Event Type	Threat	Threat Type	Scenario	Consequences	Existing Countermeasures	Vulnerability	V	T	A	$L = L_1 \times L_2$	C_1	R_1	Proposed Countermeasures
Unauthorized access.	Terrorist	I/E/C	Terrorist in VBIED defeats main gate to access the terminal.	Unauthorized access to chemicals.	1.1. Normally closed electrically operated rolling gate. 1.2. Proximity access card badge access control. 1.3. SOC controls gate, staffed 24/7. 1.4. Response by local law enforcement. 1.5. Operators may be in the area. 1.6. Security awareness and vigilance training. 1.7. Lighting.	1.1.1. Gate is not resistant to vehicle attack. 1.1.2. Police arrival at the gate may take 5 minutes. 1.1.5. No perimeter intrusion detection and surveillance system.	4	3	0.8	3	3	3	1. Increase crash resistivity of the main gate to K12. 2. Coordinate with local law enforcement to improve response time. 3. Install integrated CCTV and intrusion detection system on refinery perimeter to include access portals and waterside.
Loss of containment.	Terrorist	I/E/C	Boat borne improvised explosive device attack on barge while docked at facility during loading/ unloading.	Damage to barge and dock facilities; loss of logistics for feedstock and products; major environmental release. Fire and explosion; possible to shutdown channel.	1.1. U.S. Coast Guard boat patrols the channel and port. 1.2. Roving guard patrols. 1.3. Lighting.	1.1.1. Lack of access control from water. 1.1.2. No intrusion detection. 1.1.3. Limited CCTV surveillance of perimeter or waterside. 1.1.4. UCSG or police marine patrol arrival at the dock may take 15 minutes.	5	3	0.8	4	5	5	2. Coordinate with local law enforcement to improve response time 3. Install integrated CCTV and intrusion detection system on refinery perimeter to include access portals and waterside 4. During times of heightened threat, station a refinery security vessel at the dock during loading and unloading interdict unauthorized small craft

Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Applicable Scenarios	Residual Risk			Priority	Comments
	C_1	$L_1 \times L_2$	R_1			C_2	V_2	R_2		
Terrorist in VBIED defeats main gate to access the refinery.	3	3	3	1. Increase crash resistivity of the main gate to K12. 2. Coordinate with local law enforcement to improve response time. 3. Install integrated CCTV and intrusion detection system on refinery perimeter to include access portals and waterside.	1.1	3	2	2	2	
Boat borne improvised explosive device attack on barge while docked at facility during loading/ unloading.	5	4	5	2. Coordinate with local law enforcement to improve response time. 3. Install integrated CCTV and intrusion detection system on refinery perimeter to include access portals and waterside. 4. During times of heightened threat, station a refinery security vessel at the dock during loading and unloading to interdict unauthorized small craft.	1.2	4	3	4	1	Additional training may also be required for security officers manning the security interdiction vessel.

Alternate Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Residual Risk			Comments
	C_1	$L_1 \times L_2$	R_1		C_2	V_2	R_2	
Terrorist in VBIED defeats main gate to access the refinery.	3	3	3	1. Increase crash resistivity of the main gate to K12. 2. Coordinate with local law enforcement to improve response time. 3. Install integrated CCTV and intrusion detection system on refinery perimeter, to include access portals and waterside.	3	2	2	
Boat borne improvised explosive device attack on barge while docked at facility during loading/ unloading.	5	4	5	2. Coordinate with local law enforcement to improve response time. 3. Install integrated CCTV and intrusion detection system on refinery perimeter to include access portals and waterside. 4. During times of heightened threat, station a refinery security vessel at the dock during loading and unloading to interdict unauthorized small craft.	4	3	4	Additional training may also be required for security officers manning the security interdiction vessel.

Optional Form 6: Proposed Countermeasure Risk Reduction Score and Priority																
Proposed Countermeasures	**Applicable Scenarios—Reference Numbers**	**VH**	**H**	**M**	**L**	**VL**	R_1 **Risk Score**	**VH**	**H**	**M**	**L**	**VL**	R_2 **Risk Score**	**Risk Reduction**	**Overall Priority**	**Comments**
4. During times of heightened threat, station a refinery security vessel at the dock during loading and unloading to interdict unauthorized small craft.	1.2	5					5		4				4	1	1	Because this countermeasure could reduce both severity of consequence and likelihood of event occurrence, the team assigned it the highest priority.
3. Install integrated CCTV and intrusion detection system on refinery perimeter to include access portals and waterside.	1.1; 1.2	5	3				8		4		2		6	2	2	
2. Coordinate with local law enforcement to improve response time.	1.1; 1.2	5	3				3		4		2		6	2	3	
1. Increase crash resistivity of the main gate to K12.	1.1		3				3				2		2	1	4	

C.2.4 Example 3: Pipeline

C.2.4.1 General

The application of the API SRA methodology to a typical petroleum liquids pipeline system is illustrated in the following example and in Figure C.4. Only the first page of each of the forms is shown for illustrative purposes. It is assumed that the study is conducted by the pipeline company and the various interfaces with customers and suppliers are evaluated but the responsibility for security of those facilities is on the owners.

C.2.4.2 Form 1—Characterization Form

All entry points to the facility—gates, turnstiles, access control portals, and doors—should be evaluated as pathways in order to focus the analysis on the need for perimeter security and access control. Determine the major assets of the facility including process units, control rooms, tankage, truck and rail bays, marine loading or unloading points, communications networks, pipeline manifolds, utilities, and supporting infrastructure (e.g. motor control centers, vapor recovery units, raw water intake, electrical power, process air and steam, etc.).

— Column 1 is for the team to list all relevant assets. Similar assets within a facility with similar geographic locations on the property, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set.

— Column 2 is the type of asset (pathway, asset, activity).

— Column 3 is to document the function of the asset, pathway, or activity.

— Column 4 is to document the infrastructure/dependence and interdependence of the asset.

— Columns 5a, 5b, 5c, 5d, and 5e are for rating (VL-L-M-H-VH) the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen (this is a maximum expected damage screening assessment for casualties, environment, replacement cost, business interruption, and damage to reputation).

— Column 6 may be used to summarize ratings from Column 5a through Column 5d and to further document any asset-specific consequence information.

— Column 7 ranks the estimated overall severity of the loss of the asset, using a five-level severity ranking scale for consequence to determine the initial severity of consequence without consideration of any existing countermeasures (C).

C.2.4.3 Form 2—Threat Assessment

Document the threats against the facility.

— Column 1 shows the general types of threats that will be considered (possibly terrorists, disgruntled employees or contractors, criminals, or activists; but more specific or other groups can be considered as required for each facility-specific threat assessment).

— Column 2 is threat category [EXT—external (outsider), INT—internal (insider), COL—collusion (between external and internal adversaries)].

— Column 3 documents the general threat of that type against this or similar assets regionally, nationally, or worldwide.

— Column 4 documents the site-specific threat history for the facility being evaluated.

— Column 5 documents the potential actions that the threat could take.

— Column 6 documents and ranks the level of capability of the threat from insignificant to critical (I-L-M-H-C).

— Column 7 documents the threat's level of motivation and intent.

— Column 8 provides an overall threat ranking assessment,

— Column 9 provides the numeric rating per the five-point threat ranking scale.

C.2.4.4 Form 3—Attractiveness Assessment

— Column 1 (assets) and Column 3 (asset severity ranking) are repeated from Form 1 for reference.

— Column 2 is a documented rationale for why the particular asset is attractive (or unattractive) to each applicable threat.

— Columns 2a1, 2b1, 2c1, 2d1, etc. reflect the rationale for the ranking, and Columns 2a2, 2b2, 2c2, 2d2, etc. are the ranking of that related attractiveness on a five-point relative attractiveness ranking scale. This is repeated for each of the other credible threats.

— Column 4 is an overall TR per the five-point scale and is considered to be the highest attractiveness of any of the individual threat rankings but also considers that the sum of the different threats' interests may make the asset even more attractive. The TR is used to judge the degree of attractiveness of the target considering all the threats. It is used to identify the assets with the highest aggregate unconditional threat profile.

C.2.4.5 Form 4—Vulnerability Assessment and Risk Evaluation

— Column 1 is the security event type (common security events including unauthorized access, loss of containment, degradation of the asset, theft, contamination, disruption of operations, etc.).

— Column 2 is the threat category (threat type such as terrorist, disgruntled individual, criminal, or activist).

— Column 3 is the type of threat (insider/external/collusion).

— Column 4 describes the malevolent scenario that the identified threat perpetrates to attack the identified critical asset.

— Column 5 describes the consequences of destruction, loss, or theft of the asset.

— Column 6 captures the existing safeguards/countermeasures, which consider the strategies to deter, detect, delay, and respond.

— Column 7 captures the vulnerability of the critical asset to the postulated scenario taking into account the existing countermeasures (Column 6).

— Column 8 is the ranking of vulnerability (Column 7) as likelihood of attack success (L_2 = V), using the likelihood scale 1 to 5.

— Column 9 is the scenario-specific consequence (from Column 5), using the severity scale 1 to 5.

— Column 10 is the threat (T) number imported from the threat worksheet, using the threat scale 1 to 5.

— Column 11 is the attractiveness (A) number imported from the attractiveness worksheet, using the attractiveness scale 1 to 5 captured as a decimal value 0.0 to 1.0

— Column 12 is the calculation for overall likelihood, which includes $L_1 \times L_2$ [$T \times A$ (Column 10 × Column 11)] times vulnerability (V).

— Column 13 is the mitigated risk (R_1) to the asset, derived from plotting L_1 (Column 12) times V (L_2—in Column 8) on the likelihood axis and C_1 (Column 10) on the consequence severity axis of the SRA risk matrix to yield a color and a corresponding 1 to 5 risk number.

— If additional measures are needed to reduce the risk to a more acceptable level, Column 14 captures the recommended scenario-specific security upgrades and countermeasures proposed by the team.

C.2.4.6 Form 5—Proposed Recommendations and Residual Risk

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 documents all the places in the SRA where that specific recommendation is identified as necessary to reduce risk.

— Column 7 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 8 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 9 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 7) and V_2 (Column 8).

— Column 10 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 11 captures any additional comments.

C.2.4.7 Alternate Form 5—Determine Residual Risk Based on Implementation of All Proposed Countermeasures

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 7 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 8 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 6) and V_2 (Column 7).

— Column 9 captures any additional comments.

C.2.4.8 Optional Form 6 (if Alternate Form 5 is Used)—Proposed Countermeasure Risk Score and Priority Form

— Column 1 identifies each unique proposed additional security upgrade or countermeasure.

- Column 2 provides the reference number for each scenario within the SRA where the countermeasure in Column 1 is recommended.
- Columns 3a, 3b, 3c, 3d, and 3e capture the initial risk (R_1) across a scenarios before the recommendation was implemented.
- Column 4 presents a mathematical total of all R_1 exposures where the recommendation was to be applied to reduce risk.
- Columns 5a, 5b, 5c, 5d, and 5e capture the residual risk (R_2) across all scenarios after the recommendation was implemented.
- Column 6 presents a mathematical total of all R_2 residual exposures where the recommendation was implemented to reduce risk.
- Column 7 reflects the expected overall "risk reduction" from R_1 to R_2 if the proposed recommendation is implemented.
- Column 8 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.
- Column 9 captures any additional comments.

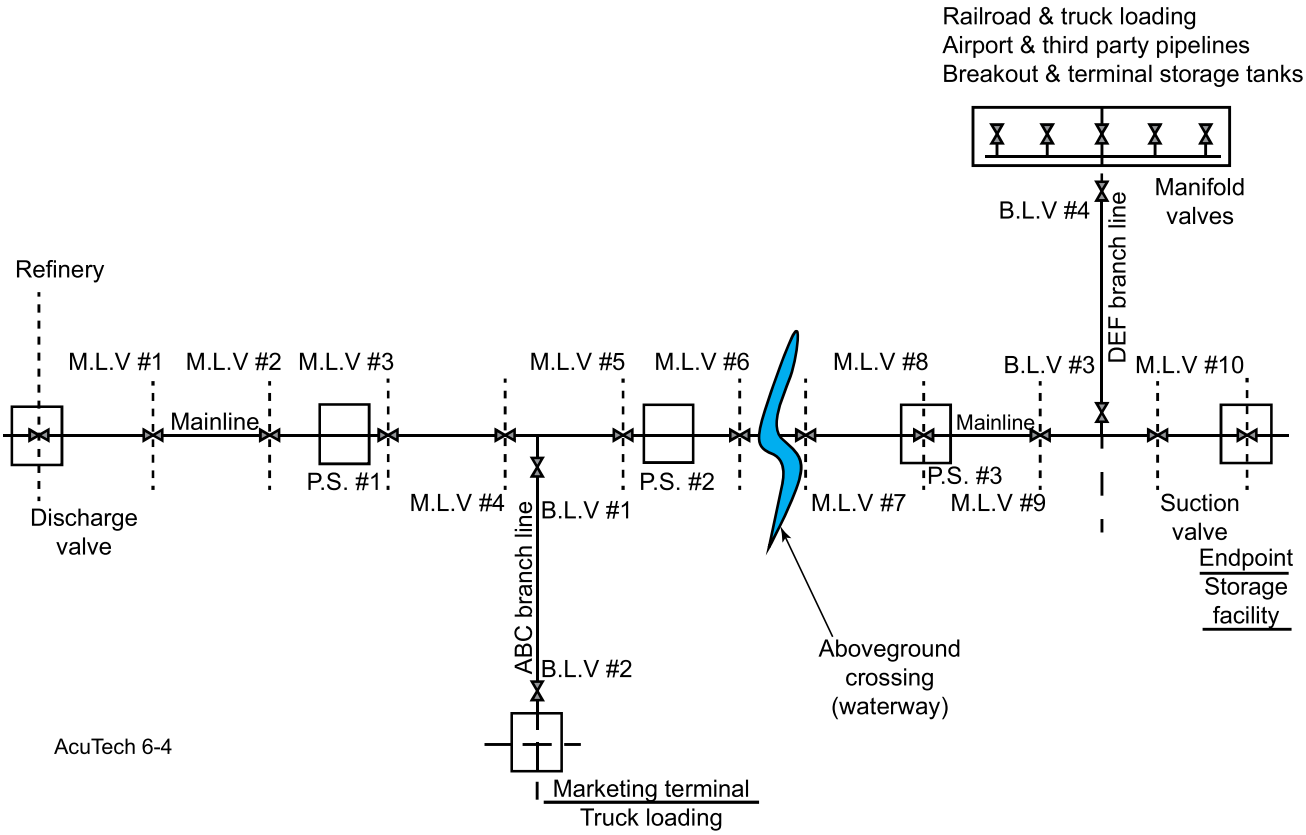

Figure C.4—Example Pipeline Diagram

Date: Facility/Operation: Reference:	Form 1—Characterization Analyze Assets and Criticality; Determine Target Assets									
Assets	**Asset Type**	**Function**	**Infrastructure Interdependence**	**Casualties**	**Environment**	**Replacement**	**Business**	**Reputation**	**Consequence**	**Asset Severity Ranking**
1. Main line	Asset	24-in. Liquids Pipeline System—1000 miles, provides 500,000 b/d. Finished products; gasoline, jet fuel, and home heating oil.	35 main-line block valves (approximately every 50 miles), 20 booster (pumping) stations, traverses primarily rural areas.	1	5	2	3	3	Main line serves large metropolitan areas. Several million retail customers plus 5 major international airports and 2 large military installations. Includes a major aboveground river crossing, which provides drinking water to large urban community.	5
2. ABC branch.	Asset	10 miles, 8-in. branch line serving mixed products to marketing terminal serving a rural population.		1	1	1	1	1	Serves rural customer base. No national defense impact. Remotely located and no major environmental impacts. Alternative delivery sources available.	1
6. River span pipeline (aboveground).	Asset	Pipeline		1	5	2	4	2	Aboveground river span. Breach could release significant product into river and contaminate public water supply to a major metropolitan center. Block valve used as active mitigation, if not damaged. Significant public safety concern due to frequent recreational and commercial use on river. Long-term repair timeframe and significant repair costs and spill clean-up costs. No alternate mode to market. Significant service interruption.	5
7. Inter-modal terminal.	Asset	Terminal		1	4	3	3	2	Large inter-modal products terminal with rail, truck and pipeline service. Serves large metropolitan area. Provides gasoline to retail market, jet fuel to 2 major international airports and USAF. Large-scale damage would take months to repair. Repair costs would be significant. Significant disruption to local economy and possible national defense. No significant environmental impact.	4

Form 2—Threat Assessment

Analyze Critical Threats

Threat	Category	General Threat History	Site-specific Threat History	Potential Actions	Threat Capability	Threat Motivation/Intent	Overall Assessment	Threat Ranking
1. International terrorists.	I/E/C	There have been numerous international terrorist acts against petroleum pipelines in the world to date. Most notably in South America and Middle East.	No site-specific history of international terrorism.	Use of stealth or force to cause damage and/or release of hydrocarbons. Possible theft or contamination of product possible but not likely. Degradation of assets and interruption of service biggest concern.	High level of organizational support; good resources; good financial backing; network of members; highly developed communication capabilities; weapons including small arms and explosives; possible vehicle bomb based on past events.	Assume adversary is highly motivated, likely extremist, prepared to die for their cause with intent to cause maximum damage to company assets including loss of life and economic disruption.	High	4
2. Domestic terrorist or activist.	I/E/C	No confirmed domestic acts of terrorism on the pipeline infrastructure.	History at the main-line system of multiple bomb threats over the past 2 years. All concluded were fakes.	Possible for a disruptive event from domestic terrorist such as bombing or disruption of operations.	Low level of organizational support; poor resources and financial backing; small network of members; cell phone/email communication capabilities; weapons including small arms and explosives.	Adversary intent is to cause economic harm through service interruption. If domestic terrorist, intent and motivation could be extreme to cause maximum damage, possibly without personal sacrifice.	Medium	3
3. Disgruntled employee or contractor.	INT	Minimal acts of sabotage or workplace violence.	No evidence of sabotage has been discovered in the past.	Sabotage to SCADA; possible release of hazardous materials, contamination of products, environmental impact, or major equipment damage.	Insider access, knowledge and ability to operate independently with authorization and without question. May have access to keys, passwords, gate access codes, comm. equipment, records, vehicles.	Nuisance adversary is intent to cause inconvenience and financial impacts to the company or their employer. If very disgruntled or troubled, intent and motivation could be extreme to cause maximum damage.	High	4

Form 3—Attractiveness Assessment

Determine Target Attractiveness Against a Specific Threat

Assets	Asset Attractiveness														Asset Severity Ranking	Target Ranking
	Threats															
	Threat 1		Threat 2		Threat 3		Threat 4		Threat 5		Threat 6		Threat 7			
	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*		
1. Main line.	Easy access because of length of pipeline and location in a rural area with several aboveground, unmanned pumping stations. Disruptions to only a rural customer base no impact to military.	1	Some insider insight helpful but not necessary.	2	Limited interest.	2									5	2
2. ABC branch.	Major disruption to residential, air travel, and military. Public safety and drinking water contamination.	2	Some insider insight helpful but not necessary.	2	Public image impact due to press/ media interest.	3									1	3
6. River span pipeline (aboveground).	Public safety and drinking water contamination. Easy access.	3	No insider knowledge needed for breach/ access.	1	Public image impact due to press/ media interest.	3									5	3

Form 4—Vulnerability Assessment and Risk Evaluation

Conduct Scenario Analysis and Assess Risk Against Security Criteria

Security Event Type	Threat	Threat Type	Scenario	Consequences	Existing Countermeasures	Vulnerability	V	T	A	$L = L_1 \times L_2$	C_1	R_1	Proposed Countermeasures
Destruction of span, release of product, and loss of containment.	Terrorist	I/E/C	Terrorist uses satchel charge to destroy piping.	Damage of river span; release of product into river; contamination of public drinking water supply; loss of service to downstream facilities for an extended period.	1.1. Fencing. 1.2. Air patrol and ground observation.	1.1.1. There is no remote CCTV or intrusion detection on the river span. 1.1.2. Law enforcement may take as long as 45 minutes to respond to a security event on the river span pipeline.	4	4	0.6	3	5	4	1. Install integrated CCTV and intrusion detection system on the river span. 2. Coordinate with local law enforcement to improve response time.
Destruction of inter-modal terminal manifold piping.	Terrorist	I/E/C	Terrorist uses satchel charge to destroy piping.	Inability to receive or pump product and possible on-site fatalities.	1.1 Fencing around cable platform. 1.2. Lighting. 1.3. Access control. 1.4. CCTV. 1.5. Staffed 24/7. 1.6. Security procedures are in place.	1.1.1. Law enforcement may take as long as 45 minutes to respond to a security event on the river span pipeline.	2	4	0.6	2	4	3	2. Coordinate with local law enforcement to improve response time.

Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Applicable Scenarios	Residual Risk			Priority	Comments
	C_1	$L_1 \times L_2$	R_1			C_2	V_2	R_2		
Terrorist uses satchel charge to destroy piping.	5	3	4	1. Install integrated CCTV and intrusion detection system on the river span. 2. Coordinate with local law enforcement to improve response time.	1.1	5	2	4	2	
Terrorist uses satchel charge to destroy piping.	4	3	4	2. Coordinate with local law enforcement to improve response time.	1.2	4	2	3	1	

Alternate Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Residual Risk			Comments
	C_1	$L_1 \times L_2$	R_1		C_2	V_2	R_2	
Terrorist uses satchel charge to destroy piping.	5	3	4	1. Install integrated CCTV and intrusion detection system on the river span. 2. Coordinate with local law enforcement to improve response time.	5	2	4	
Terrorist uses satchel charge to destroy piping.	4	3	4	2. Coordinate with local law enforcement to improve response time.	4	2	3	

Optional Form 6: Proposed Countermeasure Risk Reduction Score and Priority

Proposed Countermeasures	Applicable Scenarios—Reference Numbers	VH	H	M	L	VL	R_1 Risk Score	VH	H	M	L	VL	R_2 Risk Score	Risk Reduction	Overall Priority	Comments
2. Coordinate with local law enforcement to improve response time.	1.1; 1.2		8				8		4	3			7	1	1	
1. Install integrated CCTV and intrusion detection system in the river span.	1.1		4				4		4				4	0	2	

C.2.5 Example 4: Truck Transportation

C.2.5.1 General

The application of the API SRA methodology to a typical products distribution system by truck is illustrated in the following example and in Figure C.5. Only the first page of each of the forms is shown for illustrative purposes.

The example is of a fictitious hydrocarbon tank truck transportation system, which includes the tank truck, inventory of flammable liquids, and the route specific variables including type of road, population and environmental receptors, and any stops. It is assumed that the shipper's and receiver's sites will have a separate SRA that follows the standard facility SRA methodology. This example is intended to provide some insight on how one might conduct a security vulnerability analysis (SRA) by using this methodology on the fictitious truck transportation system. This example is not intended to be all inclusive of every situation or every item that one may consider when conducting a SRA on a tank truck system. It is recognized that not all tank truck systems are the same. Factors such as route length, type of material transported, geographic location, and many other factors play a significant role in determine the criticality of the transportation system thereby defining the type and level of analysis that may be appropriate for a particular situation.

C.2.5.2 Form 1—Characterization Form

- Column 1 is for the team to list all relevant assets. Similar assets within a facility with similar geographic locations on the property, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set.
- Column 2 is the type of asset (pathway, asset, activity).
- Column 3 is to document the function of the asset, pathway, or activity.
- Column 4 is to document the infrastructure/dependence and interdependence of the asset.
- Columns 5a, 5b, 5c, 5d, and 5e are for rating (VL-L-M-H-VH) the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen (this is a maximum expected damage screening assessment for casualties, environment, replacement cost, business interruption, and damage to reputation).
- Column 6 may be used to summarize ratings from Column 5a through Column 5d and to further document any asset-specific consequence information.
- Column 7 ranks the estimated overall severity of the loss of the asset, using a five-level severity ranking scale for consequence to determine the initial severity of consequence without consideration of any existing countermeasures (C).

C.2.5.3 Form 2—Threat Assessment

Document the threats.

- Column 1 shows the general types of threats that will be considered (possibly terrorists, disgruntled employees or contractors, criminals, or activists; but more specific or other groups can be considered as required for each facility-specific threat assessment).
- Column 2 is threat category [EXT—external (outsider), INT—internal (insider), COL—collusion (between external and internal adversaries)].
- Column 3 documents the general threat of that type against this or similar assets regionally, nationally, or worldwide.
- Column 4 documents the site-specific threat history for the facility being evaluated.

— Column 5 documents the potential actions that the threat could take.

— Column 6 documents and ranks the level of capability of the threat from insignificant to critical (I-L-M-H-C).

— Column 7 documents the threat agent's level of motivation and intent.

— Column 8 provides an overall threat ranking assessment.

— Column 9 provides the numeric rating per the five-point threat ranking scale.

C.2.5.4 Form 3—Attractiveness Assessment

— Column 1 (assets) and Column 3 (asset severity ranking) are repeated from Form 1 for reference.

— Column 2 is a documented rationale for why the particular asset is attractive (or unattractive) to each applicable threat.

— Columns 2a1, 2b1, 2c1, 2d1, etc. reflect the rationale for the ranking, and Columns 2a2, 2b2, 2c2, 2d2, etc. are the ranking of that related attractiveness on a five-point relative attractiveness ranking scale. This is repeated for each of the other credible threats.

— Column 4 is an overall TR per the five-point scale, and is considered to be the highest attractiveness of any of the individual threat rankings but also considers that the sum of the different threats' interests may make the asset even more attractive. The target ranking is used to judge the degree of attractiveness of the target considering all the threats. It is used to identify the assets with the highest aggregate unconditional threat profile.

C.2.5.5 Form 4—Vulnerability Assessment and Risk Evaluation

— Column 1 is the security event type (common security events including unauthorized access, loss of containment, degradation of the asset, theft, contamination, disruption of operations, etc.).

— Column 2 is the threat category (threat type such as terrorist, disgruntled individual, criminal, or activist).

— Column 3 is the type of threat (insider/external/collusion).

— Column 4 describes the malevolent scenario that the identified threat perpetrates to attack the identified critical asset.

— Column 5 describes the consequences of destruction, loss, or theft of the asset.

— Column 6 captures the existing safeguards/countermeasures, which consider the strategies to deter, detect, delay, and respond.

— Column 7 captures the vulnerability of the critical asset to the postulated scenario taking into account the existing countermeasures (Column 6).

— Column 8 is the ranking of vulnerability (Column 7) as likelihood of attack success (L_2 = V), using the likelihood scale 1 to 5.

— Column 9 is the scenario-specific consequence (from Column 5), using the severity scale 1 to 5.

— Column 10 is the threat (T) number imported from the threat worksheet, using the threat scale 1 to 5.

— Column 11 is the attractiveness (A) number imported from the attractiveness worksheet, using the attractiveness scale 1 to 5 captured as a decimal value 0.0 to 1.0.

— Column 12 is the calculation for overall likelihood, which includes $L_1 \times L_2$ [$T \times A$ (Column 10 × Column 11)] times vulnerability (V).

— Column 13 is the mitigated risk (R_1) to the asset, derived from plotting L_1 (Column 12) times V (L_2—in Column 8) on the likelihood axis and C_1 (Column 10) on the consequence severity axis of the SRA risk matrix to yield a color and a corresponding 1 to 5 risk number.

— If additional measures are needed to reduce the risk to a more acceptable level, Column 14 captures the recommended scenario-specific security upgrades and countermeasures proposed by the team.

C.2.5.6 Form 5—Proposed Recommendations and Residual Risk

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 documents all the places in the SRA where that specific recommendation is identified as necessary to reduce risk.

— Column 7 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 8 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 9 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 7) and V_2 (Column 8).

— Column 10 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 11 captures any additional comments.

C.2.5.7 Alternate Form 5—Determine Residual Risk Based on Implementation of All Proposed Countermeasures

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 7 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 8 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 6) and V_2 (Column 7).

— Column 9 captures any additional comments.

C.2.5.8 Optional Form 6 (if Alternate Form 5 is Used)—Proposed Countermeasure Risk Score and Priority Form

— Column 1 identifies each unique proposed additional security upgrade or countermeasure.

— Column 2 provides the reference number for each scenario within the SRA where the countermeasure in Column 1 is recommended.

— Columns 3a, 3b, 3c, 3d, and 3e capture the initial risk (R_1) across a scenarios before the recommendation was implemented.

— Column 4 presents a mathematical total of all R_1 exposures where the recommendation was to be applied to reduce risk.

— Columns 5a, 5b, 5c, 5d, and 5e capture the residual risk (R_2) across all scenarios after the recommendation was implemented.

— Column 6 presents a mathematical total of all R_2 residual exposures where the recommendation was implemented to reduce risk.

— Column 7 reflects the expected overall "risk reduction" from R_1 to R_2 if the proposed recommendation is implemented

— Column 8 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 9 captures any additional comments.

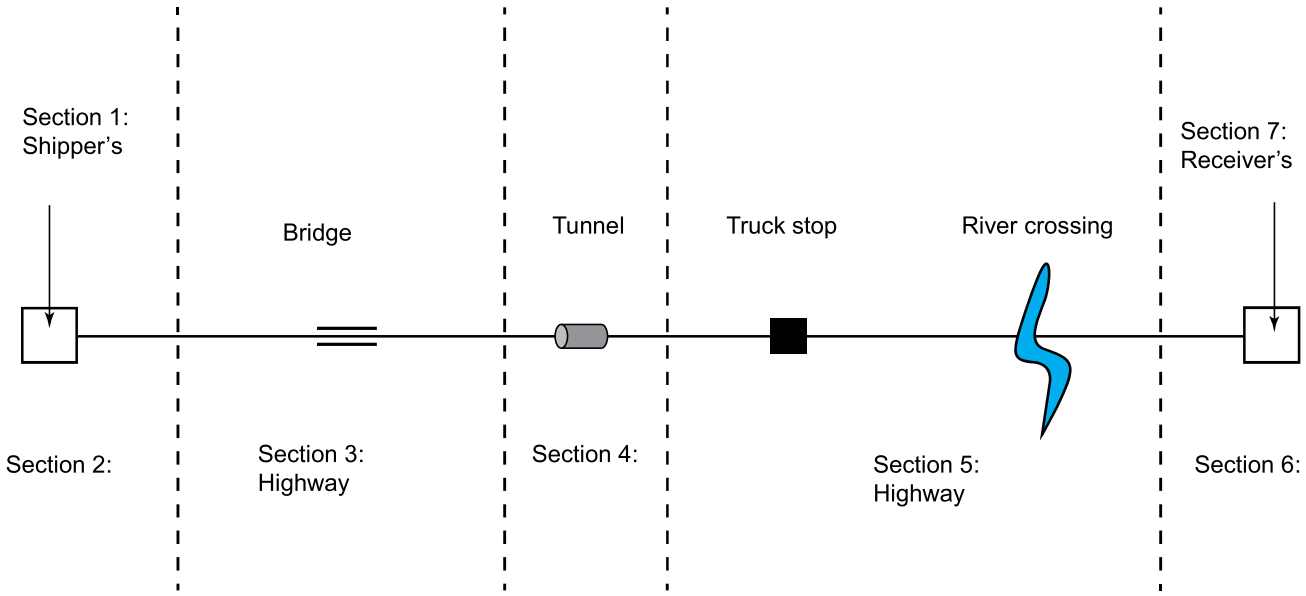

Figure C.5—Example Truck Transportation Diagram

Date: Facility/Operation: Reference:	Form 1—Characterization Analyze Assets and Criticality; Determine Target Assets									
Assets	**Asset Type**	**Function**	**Infrastructure Interdependence**	**Casualties**	**Environment**	**Replacement**	**Business**	**Reputation**	**Consequence**	**Asset Severity Ranking**
1. Tank truck.	Asset	Contains petroleum products and conducts loading rack operations.	Shipper loads 50 tank trucks per day of products and dispatches them to both local receivers and to within nearby neighboring states. Route evaluated is the longest distance transported to a receiver's site.	3	3	2	3	3	Potential for flammable liquids to be attacked directly to damage the loading rack and operations, to be attacked while en route to cause collateral damage, or to be hijacked and used as a weapon against other targets.	3
2. Rural section of road leading from the shipper's site to HWY 100.	Asset	15 miles, traversing primarily rural areas.	Single entrance/exit to supplier's site.	1	2	1	1	2	Incident involving tank truck on this section of route would result in limited impacts due to low population density.	2
3. HWY 100.	Asset	50 miles, traversing primarily through rural areas.	Long stretch across rural section of route.	1	2	1	1	2	Incident involving tank truck on this section of route would result in limited impacts due to low population density.	2
1. Tank truck.	Asset	Contains petroleum products and conducts loading rack operations.	Shipper loads 50 tank trucks per day of products and dispatches them to both local receivers and to within nearby neighboring states. Route evaluated is the longest distance transported to a receiver's site.	3	3	2	3	3	Potential for flammable liquids to be attacked directly to damage the loading rack and operations, to be attacked while en route to cause collateral damage, or to be hijacked and used as a weapon against other targets.	3

Form 2—Threat Assessment

Analyze Critical Threats

Threat	Category	General Threat History	Site-specific Threat History	Potential Actions	Threat Capability	Threat Motivation/Intent	Overall Assessment	Threat Ranking
1. Terrorist.	EXT	According to information bulletins from the U.S. Department of Homeland Security (DHS), there have been suspicious activities involving bulk facilities including surveillance and following trucks. International terrorists have targeted trucks for hijackings and direct attacks.	No site-specific history of intentional acts against the company.	Use of force to cause damage to vehicles while in transit or at loading/offloading facilities. This could cause a release of hydrocarbons and resulting fire and explosion with possible fatalities and injuries and degradation of transportation assets and environmental release.	Assume a high level of organizational support; good resources; good financial backing; network of members; highly developed communication capabilities; weapons including small arms and explosives; possible vehicle bomb based on past events.	Assume adversary is highly motivated, likely extremist, prepared to die for their cause with intent to cause maximum damage to company assets including loss of life and economic disruption.	Medium	3
2. Domestic terrorist or activist.	I/E/C	No confirmed domestic acts of terrorism against fuels trucking operations.	History of bomb threats against company. Company has had activist protest at the main gate within the past 2 years.	Possible for a disruptive event from domestic terrorist such as bombing or disruption of operations. Possible actions would include hijackings, theft, vandalism, and arson.	Assume medium level of organizational support; poor resources and financial backing; small network of members; cell phone/email communication capabilities; weapons including small improvised explosive devices.	Adversary intent is to cause economic harm through service interruption or to emphasize a political cause. If domestic terrorist, intent and motivation could be extreme to cause maximum damage, but more likely without personal sacrifice.	Medium	3
3. Disgruntled employee or contractor.	INT	There have been acts of sabotage, theft, and arson to the petroleum trucking operations in the past.	No evidence of sabotage has been discovered in the past.	Sabotage to vehicles, including safety systems, arson, and theft of product.	Insider access, knowledge and ability to operate independently with authorization and without question.	Disgruntled employee is most likely intent to cause inconvenience and financial impacts to the company or their employer.	Low	2

Form 3—Attractiveness Assessment

Determine Target Attractiveness Against a Specific Threat

Assets	Asset Attractiveness														Asset Severity Ranking	Target Ranking
	Threats															
	Threat 1		Threat 2		Threat 3		Threat 4		Threat 5		Threat 6		Threat 7			
	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*		
1. Tank truck.	Potential for release resulting in large fire, potential fatalities, and closure/ damage to major transportation route.	3	Insider information necessary to gain access to vehicle.	1	Public image impact due to press/ media interest.	2									3	3
2. Rural section of road from the shipper's site to HWY 100.															2	2
2. HWY 100.															2	2
4. Downtown section of route along State Route 5.	High population density and potential to harm a large number of people.	3	No additional attraction.	1	No additional attraction.	1									3	3

Form 4—Vulnerability Assessment and Risk Evaluation

Conduct Scenario Analysis and Assess Risk Against Security Criteria

Security Event Type	Threat	Threat Type	Scenario	Consequences	Existing Countermeasures	Vulnerability	V	T	A	$L = L_1 \times L_2$	C_1	R_1	Proposed Countermeasures
1.1. Truck is attacked en route resulting in a release of hydrocarbons.	Terrorist	I/E/C	Release and ignition of hydrocarbons on a major roadway.	Potential fatalities and injuries from resulting fire. Possible closure of a major transportation route.	1.1. Experienced/ Licensed Drivers—Background checks before employment. 1.2. Identification of driver's checked at both the shipper's and receiver's site. 1.3. Drivers trained in HAZMAT. 1.4. Truck is in constant radio contact while en route.	1.1.1. Longest route exposes the truck many hours per shipment; provides the opportunity for surveillance and unexpected attack; route also passes along several areas of high population density and included bridges and tunnels. No real-time tracking capability to assist response	4	3	0.6	3	3	3	Install real time GPS tanker tracking annunciated in a regional or national SOC to monitor tanker security and provide for timely response.
1.2. Truck is hijacked en route.	Terrorist	I/E/C	Theft of truck and product.	Potential for injury/fatality to driver in an attack by force. Loss of truck and product, but unlikely to be used in subsequent attack.	2.1. Truck is in constant radio contact while en route. 2.2. Single scheduled truck stop along route. 2.3. Truck is normally locked when driver is at the truck stop. 2.4. Truck has electronic disengagement systems.	2.1.1. Long stretches of rural areas along route provide opportunity for surveillance and attack; truck is left unattended while at the truck stop.	3	3	0.6	2	2	2	

Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Applicable Scenarios	Residual Risk			Priority	Comments
	C_1	$L_1 \times L_2$	R_1			C_2	V_2	R_2		
Truck is attacked en route resulting in a release of hydrocarbons.	3	3	3	1. Install real time GPS tanker tracking annunciated in a regional or national SOC to monitor tanker security and provide for timely response.	1.1	3	2	2	1	
Truck is hijacked en route.	2	2	2							Risk is acceptable, no additional countermeasures are required.

Alternate Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Residual Risk			Comments
	C_1	$L_1 \times L_2$	R_1		C_2	V_2	R_2	
Truck is attacked en route resulting in a release of hydrocarbons.	3	3	3	1. Install real time GPS tanker tracking annunciated in a regional or national SOC to monitor tanker security and provide for timely response.	3	2	2	
Truck is hijacked en route.	2	2	2					Risk is acceptable, no additional countermeasures are required.

Optional Form 6: Proposed Countermeasure Risk Reduction Score and Priority

Proposed Countermeasures	Applicable Scenarios—Reference Numbers	VH	H	M	L	VL	R_1 Risk Score	VH	H	M	L	VL	R_2 Risk Score	Risk Reduction	Overall Priority	Comments
1. Install real time GPS tanker tracking annunciated in a regional or national SOC to monitor tanker security and provide for timely response.	1.1			3			3				2		2	1	1	

C.2.6 Example 5: Rail Transportation

C.2.6.1 General

The application of the API SRA methodology to a typical rail transportation system value chain is conducted as illustrated in the following forms and in Figure C.6. Only the first page of each of the forms is shown for illustrative purposes. In this example, it is assumed that the study is conducted by the shipper company and the various interfaces with customers and suppliers are evaluated, but the responsibility for security of those facilities is on the owners. This approach would be useful for both understanding the risks of interfaces that the shipper owns and operates, as well as the general route risk assessment issues.

C.2.6.2 Form 1—Characterization Form

— Column 1 is for the team to list all relevant assets. Similar assets within a facility with similar geographic locations on the property, common vulnerabilities, and common consequences can be grouped for efficiency and to consider the value of an entire functional set.

— Column 2 is the type of asset (pathway, asset, activity).

— Column 3 is to document the function of the asset, pathway, or activity.

— Column 4 is to document the infrastructure/dependence and interdependence of the asset.

— Columns 5a, 5b, 5c, 5d, and 5e are for rating (VL-L-M-H-VH) the hazards and consequences that would be realized if the asset was damaged, compromised, or stolen (this is a maximum expected damage screening assessment for casualties, environment, replacement cost, business interruption, and damage to reputation).

— Column 6 may be used to summarize ratings from Column 5a through Column 5d and to further document any asset-specific consequence information.

— Column 7 ranks the estimated overall severity of the loss of the asset, using a five-level severity ranking scale for consequence to determine the initial severity of consequence without consideration of any existing countermeasures (C).

C.2.6.3 Form 2—Threat Assessment

Document the threats.

— Column 1 shows the general types of threats that will be considered (possibly terrorists, disgruntled employees or contractors, criminals, or activists; but more specific or other groups can be considered as required for each facility-specific threat assessment).

— Column 2 is threat category [EXT—external (outsider), INT—internal (insider), COL—collusion (between external and internal adversaries)].

— Column 3 documents the general threat of that type against this or similar assets regionally, nationally, or worldwide.

— Column 4 documents the site-specific threat history for the facility being evaluated.

— Column 5 documents the potential actions that the threat could take.

— Column 6 documents and ranks the level of capability of the threat from insignificant to critical (I-L-M-H-C).

— Column 7 documents the threat's level of motivation and intent.

— Column 8 provides an overall threat ranking assessment.

— Column 9 provides the numeric rating per the five-point threat ranking scale.

C.2.6.4 Form 3—Attractiveness Assessment

— Column 1 (assets) and Column 3 (asset severity ranking) are repeated from Form 1 for reference.

— Column 2 is a documented rationale for why the particular asset is attractive (or unattractive) to each applicable threat.

— Columns 2a1, 2b1, 2c1, 2d1, etc. reflect the rationale for the ranking, and Columns 2a2, 2b2, 2c2, 2d2, etc. are the ranking of that related attractiveness on a five-point relative attractiveness ranking scale. This is repeated for each of the other credible threats.

— Column 4 is an overall TR per the five-point scale, and is considered to be the highest attractiveness of any of the individual threat rankings but also considers that the sum of the different threats' interests may make the asset even more attractive. The target ranking is used to judge the degree of attractiveness of the target considering all the threats. It is used to identify the assets with the highest aggregate unconditional threat profile.

C.2.6.5 Form 4—Vulnerability Assessment and Risk Evaluation

— Column 1 is the security event type (common security events including unauthorized access, loss of containment, degradation of the asset, theft, contamination, disruption of operations, etc.).

— Column 2 is the threat category (threat type such as terrorist, disgruntled individual, criminal, or activist).

— Column 3 is the type of threat (insider/external/collusion).

— Column 4 describes the malevolent scenario that the identified threat perpetrates to attack the identified critical asset.

— Column 5 describes the consequences of destruction, loss, or theft of the asset.

— Column 6 captures the existing safeguards/countermeasures, which consider the strategies to deter, detect, delay, and respond.

— Column 7 captures the vulnerability of the critical asset to the postulated scenario taking into account the existing countermeasures (Column 6).

— Column 8 is the ranking of vulnerability (Column 7) as likelihood of attack success ($L_2 = V$), using the likelihood scale 1 to 5.

— Column 9 is the scenario-specific consequence (from Column 5), using the severity scale 1 to 5.

— Column 10 is the threat (T) number imported from the threat worksheet, using the threat scale 1 to 5.

— Column 11 is the attractiveness (A) number imported from attractiveness worksheet, using the attractiveness scale 1 to 5 captured as a decimal value 0.0 to 1.0.

— Column 12 is the calculation for overall likelihood, which includes $L_1 \times L_2$ [$T \times A$ (Column 10 × Column 11)] times vulnerability (V).

— Column 13 is the mitigated risk (R_1) to the asset, derived from plotting L_1 (Column 12) times V (L_2—in Column 8) on the likelihood axis, and C_1 (Column 10) on the consequence severity axis of the SRA risk matrix to yield a color and a corresponding 1 to 5 risk number.

— If additional measures are needed to reduce the risk to a more acceptable level, Column 14 captures the recommended scenario-specific security upgrades and countermeasures proposed by the team.

C.2.6.6 Form 5—Proposed Recommendations and Residual Risk

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 documents all the places in the SRA where that specific recommendation is identified as necessary to reduce risk.

— Column 7 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 8 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 9 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 7) and V_2 (Column 8).

— Column 10 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 11 captures any additional comments.

C.2.6.7 Alternate Form 5—Determine Residual Risk Based on Implementation of All Proposed Countermeasures

— Column 1 describes the scenario under analysis.

— Columns 2, 3, 4, and 5 are repeated from Form 4 for reference.

— Column 6 (C_2) is the new ranking of the consequences specific to the scenario, presuming the implementation of all recommendations.

— Column 7 (V_2) is the revised ranking for the likelihood of expected attack success (retaining the original value for L_1), presuming the implementation of all recommendations.

— Column 8 is the ranking for residual risk, considering the changes in consequences and likelihood achieved through the recommended countermeasures, as expressed in C_2 (Column 6) and V_2 (Column 7).

— Column 9 captures any additional comments.

C.2.6.8 Optional Form 6 (if Alternate Form 5 is Used)—Proposed Countermeasure Risk Score and Priority Form

— Column 1 identifies each unique proposed additional security upgrade or countermeasure

— Column 2 provides the reference number for each scenario within the SRA where the countermeasure in Column 1 is recommended

— Columns 3a, 3b, 3c, 3d, and 3e capture the initial risk (R_1) across a scenarios before the recommendation was implemented.

— Column 4 presents a mathematical total of all R_1 exposures where the recommendation was to be applied to reduce risk.

— Columns 5a, 5b, 5c, 5d, and 5e capture the residual risk (R_2) across all scenarios after the recommendation was implemented.

— Column 6 presents a mathematical total of all R_2 residual exposures where the recommendation was implemented to reduce risk

— Column 7 reflects the expected overall "risk reduction" from R_1 to R_2 if the proposed recommendation is implemented

— Column 8 is the assigned priority ranking of each proposed recommendation as determined by the SRA team.

— Column 9 captures any additional comments.

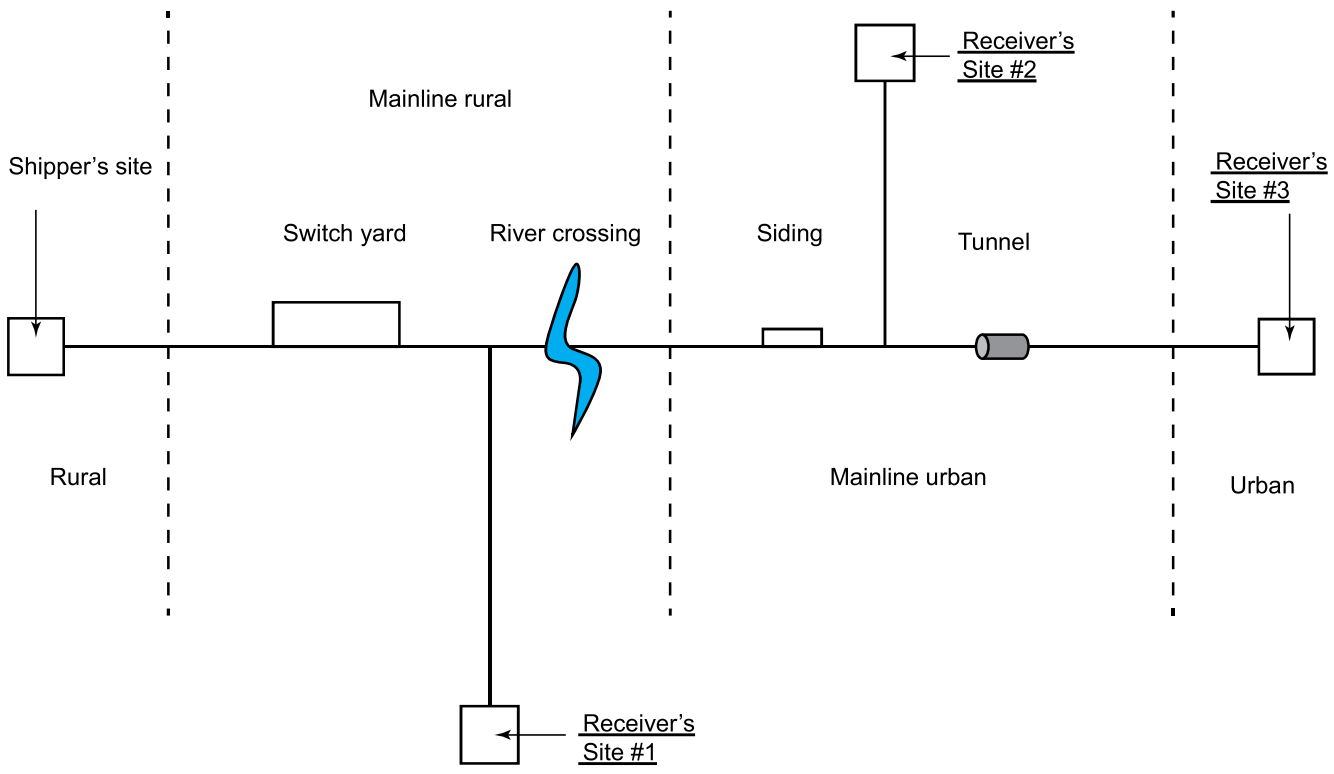

Figure C.6—Example Rail Transportation Diagram

Date: Facility/Operation: Reference:	Form 1—Characterization Analyze Assets and Criticality; Determine Target Assets									
Assets	**Asset Type**	**Function**	**Infrastructure Interdependence**	**Casualties**	**Environment**	**Replacement**	**Business**	**Reputation**	**Consequence**	**Asset Severity Ranking**
1. 25 railcars of petroleum products.	Asset	Two trains comprised solely of 25 petroleum products railcars are shipped daily from the shipper's terminal.	After leaving the terminal the tank cars are divided into three separate trains at the switch yard and sent to three final receiver's sites. Site #1—25 railcars per day. Site #2—10 railcars per day. Site #3—15 railcars. En route from the switch yard to Site #1 is on a mainline track along a mostly rural area. En route to Sites #2 and #3 crosses a river and have access to a siding as needed. The route to Site #2 branches off on an urban mainline, while the route to Site #3 continues through a tunnel before reaching its final destination.	3	3	2	2	3	Potential hazard for this route is the potential to release one or more railcars resulting in a large environmental impact and or fire and subsequent fatalities and injuries if ignited.	3
2. Rural section of track to switch yard.	Asset	25 miles from shipper's site	Single rail entrance/exit to supplier's site	2	3	2	2	3	Incident involving railcar on this section of the route would result in limited fatalities/injuries due to low population density, but large fire could damage rail line.	3
3. Mainline section of track in rural area.	Asset	200 miles. Including rail spur to Receiver Site #1.	Long stretch across rural section of route.	2	2	2	2	3	Limited potential for casualties, asset loss or environmental impact, but spill and/or fire could have impact on company reputation.	3
4. Switch yard.	Asset	Primary switching yard for trains.	Switch point to individual trains to receiver's sites.	2	3	3	3	3	Potential to damage site, other railcars, and various products if petroleum products released and ignited.	3
5. River crossing.	Asset	Railroad trestle over navigable river.		1	3	2	2	3	Potential for environmental impact if product released into river.	3

Form 2—Threat Assessment Analyze Critical Threats								
Threat	**Category**	**General Threat History**	**Site-specific Threat History**	**Potential Actions**	**Threat Capability**	**Threat Motivation/Intent**	**Overall Assessment**	**Threat Ranking**
1. Terrorist.	I/E/C	Bombings in Madrid indicated the vulnerability of the rail transportation infrastructure.	No site-specific history of intentional acts against company.	Terrorists may be interested in 1) weaponization of a train 2) directly damage the railcar(s), collateral damage and disruption 3) "Trojan Horse" attack to introduce a weapon into a facility.	Assume a high level of organizational support; good resources; good financial backing; network of members; highly developed communication capabilities; weapons including small arms and explosives; possible vehicle bomb based on past events.	Assume adversary is highly motivated, likely extremist, prepared to die for their cause with intent to cause maximum damage to company assets including loss of life and economic disruption.	Medium	3
2. Domestic terrorist or activist.	I/E/C	No confirmed domestic acts of terrorism against fuels rail operations.	History of bomb threats at company. Company has had activist protest at the corporate headquarters within the past 5 years.	Possible for a disruptive event from domestic terrorist such as bombing or disruption of operations. Possible actions would include vandalism, blockage of track, and arson.	Assume medium level of organizational support; poor resources and financial backing; small network of members; cell phone/email communication capabilities; weapons including small improvised explosive devices.	Adversary intent is to cause economic harm through service interruption or to emphasize a political cause. If domestic terrorist, intent and motivation could be extreme to cause maximum damage, but more likely without personal sacrifice.	Medium	3
3. Disgruntled employee or contractor.	INT	There have been acts of sabotage, theft, and arson to the petroleum trucking operations in the past.	No evidence of sabotage has been discovered in the past.	Sabotage to railcars including safety systems and arson.	Insider access, knowledge and ability to operate independently with authorization and without question.	Disgruntled employee is most-likely intent to cause inconvenience and financial impacts to the company or their employer.	Medium	4

Form 3—Attractiveness Assessment

Determine Target Attractiveness Against a Specific Threat

Assets	Asset Attractiveness														Asset Severity Ranking	Target Ranking
	Threats															
	Threat 1		Threat 2		Threat 3		Threat 4		Threat 5		Threat 6		Threat 7			
	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*	Rationale	*A*		
1. 25 railcars of petroleum products.	Potential for release resulting in large fire, potential fatalities, and closure/ damage to major transportation route.	3	Insider information necessary to gain access to vehicle.	1	Public image impact due to press/ media interest.	2									3	3
2. Rural section of track to switch yard.	Short section of route and limited number of potential impacts.	1	No additional attraction.	1	No additional attraction.	1									3	1
3. Mainline section of track in rural area.	Minimal attraction due to limited impact potential, but length of route provides access to vehicle.	2	No additional attraction.	1	No additional attraction.	1									3	2

Form 4—Vulnerability Assessment and Risk Evaluation

Conduct Scenario Analysis and Assess Risk Against Security Criteria

Security Event Type	Threat	Threat Type	Scenario	Consequences	Existing Countermeasures	Vulnerability	V	T	A	$L = L_1 \times L_2$	C_1	R_1	Proposed Countermeasures
1.1. Train is attacked en route with a bomb resulting in a release of petroleum products.	Terrorist	I/E/C	Release and ignition of petroleum products on a major roadway.	Possible closure/damage to major transport ion rail line and potential fatalities and injuries from resulting fire.	1.1. Major Class I Railroad used to carry materials along the entire route to all receivers' sites. 1.2. Security plan at both the shipper and receiver's site. 1.3. Train is in constant radio contact while en route.	1.1.1. Railcars are exposed many hours per shipment; provides the opportunity for surveillance and unexpected attack; route also passes along several areas of high population density and includes both bridge and tunnel. No real-time tracking capability to assist response.	4	3	0.6	3	4	3	1. Install real-time GPS rail car tracking annunciated in a regional or national SOC to monitor tanker security and provide for timely response.
1.2. Bomb is attached to railcar while in switch yard or while on siding.	Terrorist	I/E/C	Bomb is brought onto receiver's site.	Explosion/fire on the rail spurs of at the receiver's site resulting in fatalities/injuries and potential damage to spur and receivers process equipment.	2.1. Security plan at both the shipper and receiver's site.	1.2.1. Railcars are exposed and vulnerable to placement of hidden bomb on railcar while in yard and while on spur.	5	3	0.6	3	4	3	2. Establish a procedure during heightened threat for all rail cars to be thoroughly inspected before being allowed into the site.

Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Applicable Scenarios	Residual Risk			Priority	Comments
	C_1	$L_1 \times L_2$	R_1			C_2	V_2	R_2		
1.1. Train is attacked en route with a bomb resulting in a release of petroleum products.	3	4	3	1. Install real time GPS rail car tracking annunciated in a regional or national SOC to monitor tanker security and provide for timely response.	1.1	3	3	3	2	
1.2. Bomb is attached to railcar while in switch yard or while on siding.	4	4	3	2. Establish a procedure during heightened threat for all rail cars to be thoroughly inspected before being allowed into the site.	1.2	3	3	3	1	Lower cost drives this priority.

Alternate Form 5—Recommendations

Determine Residual Risk Based on Implementation of Proposed Countermeasures

Scenario	Existing Risk			Proposed Countermeasures	Residual Risk			Comments
	C_1	$L_1 \times L_2$	R_1		C_2	V_2	R_2	
1.1. Train is attacked en route with a bomb resulting in a release of petroleum products.	3	4	3	1. Install real time GPS rail car tracking annunciated in a regional or national SOC to monitor tanker security and provide for timely response.	3	3	3	
1.2. Bomb is attached to railcar while in switch yard or while on siding.	4	4	3	2. Establish a procedure during heightened threat for all rail cars to be thoroughly inspected before being allowed into the site.	3	3	3	

Optional Form 6: Proposed Countermeasure Risk Reduction Score and Priority

Proposed Countermeasures	Applicable Scenarios—Reference Numbers	VH	H	M	L	VL	R_1 Risk Score	VH	H	M	L	VL	R_2 Risk Score	Risk Reduction	Overall Priority	Comments
2. Establish a procedure during heightened threat for all rail cars to be thoroughly inspected before being allowed into the site.	1.2		4				3			3			3	0	1	Lower cost drives this priority.
	1.1; 1.2			3			3			3			3	0	2	Proposed countermeasure would improve security, but not enough to provide significant reduction in risk.

Bibliography

This standard was developed for the industry as an adjunct to other available references which includes the following.

[1] API, *Security Guidelines for the Petroleum Industry,* May 2003

[2] API Recommended Practice 70, *Security for Offshore Oil and Natural Gas Operations*, First Edition, April 2003

[3] American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, August 2002

[4] Sandia National Laboratories, *Vulnerability Analysis Methodology for Chemical Facilities (VAM-CF)*, 2002

[5] U. S. Department of Transportation Title 49, *CFR* 172 HM-232, 2005

[6] Maritime Transportation Security Act of 2002, Public Law 107-295-Nov 25, 2002

[7] U.S. Department of Homeland Security, *Chemical Facility Anti-Terrorism Standards*, 6 *CFR* Part 27, Final Rule, April 9, 2007

[8] INGAA and AGA, *Security Practices Guidelines Natural Gas Industry Transmission and Distribution*, May 2008

[9] CSA, CSA Z246.1-09, *Security Management for Natural Gas and Petroleum Industry Systems*, 2009

[10] DOT/OPS, *Pipeline Security Contingency Planning Guidance*, June 13, 2002

[11] U.S. Transportation Security Administration, *Pipeline Security Information Circular, Security Guidance for Natural Gas, and Hazardous Liquid Pipelines and Liquefied Natural Gas Facilities,* 2002

[12] ASIS, SPC-1.2009, *Organizational Resilience, Security, Preparedness, and Continuity Management Systems, Requirements with Guidance for Use*, 2009

[13] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, 2009

[14] U.S. Department of Homeland Security, Risk Steering Committee, *DHS Risk Lexicon*, 2010 Edition, September 2010

[15] ISO 31000: 2009, *Risk management—Principles and guidelines on implementation*, 2009

[16] Defense R&D Canada, Centre for Security Science, *Intelligence Experts Group All Hazards Risk Assessment Lexicon*, November 2007

[17] Joint Technical Committee OB007, Risk Management, *Australia/New Zealand Risk Management Standard 4360*, August 2004

[18] Committee for Definitions, *Society of Risk Analysis (SRA) Glossary*; estimated date, 2008

[19] Ortwin Renn (author) and Peter Graham (annexes), International Risk Governance Committee (IRGC) definitions from the white paper *Risk Governance, Towards an Integrated Approach*, January 2006

[20] ISO/IEC CD Guide 73, *Risk Management—Vocabulary*, produced by "Chemical Accident Prevention Provisions" (Title 40, *CFR* Part 68)

[21] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Chemical Facility Vulnerability Assessment Methodology,* NIJ Special Report, July 2002

[22] "Counterterrorism and Contingency Planning Guide," special publication from *Security Management Magazine and American Society for Industrial Security*, 2001

[23] U.S. Environmental Protection Agency, *General Guidance on Risk Management Programs for Chemical Accident Prevention* (40 *CFR* Part 68), 1998

[24] American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), *Guidelines for Chemical Process Quantitative Risk Analysis*, Second Edition, 2000

[25] American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), *Guidelines for Consequence Analysis of Chemical Releases*, 1999

[26] American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), *Guidelines for Technical Management of Chemical Process Safety*, 1998

[27] American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), *Guidelines for Technical Planning for On-Site Emergencies*, 1996

[28] American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), *Inherently Safer Chemical Processes—A Life Cycle Approach*, 1996

[29] American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), *Layers of Protection Analysis*, 2001

[30] American Chemistry Council, *Site Security Guidelines for the U.S. Chemical Industry*, October 2001

[31] Bowers, Dan M., "Security Fundamentals for the Safety Engineer," *Professional Safety,* American Society of Safety Engineers, December 2001, pp. 31–33

[32] Dalton, Dennis, *Security Management: Business Strategies for Success* (Newton, MA: Butterworth-Heinemann Publishing, 1995)

[33] Fischer, Robert J., and G. Green, *Introduction to Security*, Sixth Edition (Boston: Butterworth-Heinemann, 1998)

[34] Roper, C. A., *Physical Security and the Inspection Process* (Boston: Butterworth-Heinemann, 1997)

[35] Roper, C.A., *Risk Management for Security Professionals* (Boston: Butterworth-Heinemann, 1999)

[36] Walsh, Timothy J., and R. J. Healy, eds. *Protection of Assets Manual* (Santa Monica, CA: Merritt Co.). Four-volume loose-leaf reference manual, updated monthly.

[37] *Secretariat of ISO TMB WG on Risk Management*, June 2009

EXPLORE SOME MORE

Check out more of API's certification and training programs, standards, statistics and publications.

API Monogram™ Licensing Program

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: certification@api.org
Web: www.api.org/monogram

API Quality Registrar (APIQR™)

- ISO 9001
- ISO/TS 29001
- ISO 14001
- OHSAS 18001
- API Spec Q1®
- API Spec Q2™
- API Quality*Plus*™
- Dual Registration

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: certification@api.org
Web: www.api.org/apiqr

API Training Provider Certification Program (API TPCP®)

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: tpcp@api.org
Web: www.api.org/tpcp

API Individual Certification Programs (ICP™)

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: icp@api.org
Web: www.api.org/icp

API Engine Oil Licensing and Certification System (EOLCS™)

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: eolcs@api.org
Web: www.api.org/eolcs

Motor Oil Matters™

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: motoroilmatters@api.org
Web: www.motoroilmatters.org

API Diesel Exhaust Fluid™ Certification Program

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: apidef@api.org
Web: www.apidef.org

API Perforator Design™ Registration Program

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: perfdesign@api.org
Web: www.api.org/perforators

API WorkSafe™

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: apiworksafe@api.org
Web: www.api.org/worksafe

API-U®

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: training@api.org
Web: www.api-u.org

API eMaintenance™

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: apiemaint@api.org
Web: www.apiemaintenance.com

API Standards

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Email: standards@api.org
Web: www.api.org/standards

API Data™

Sales: 877-562-5187
(Toll-free U.S. and Canada)
(+1) 202-682-8041
(Local and International)
Service: (+1) 202-682-8042
Email: data@api.org
Web: www.api.org/data

API Publications

Phone: 1-800-854-7179
(Toll-free U.S. and Canada)
(+1) 303-397-7956
(Local and International)
Fax: (+1) 303-397-2740
Web: www.api.org/pubs
global.ihs.com

AMERICAN PETROLEUM INSTITUTE

1220 L Street, NW
Washington, DC 20005-4070
USA

202-682-8000

Additional copies are available online at www.api.org/pubs

Phone Orders:	1-800-854-7179	(Toll-free in the U.S. and Canada)
	303-397-7956	(Local and International)
Fax Orders:	303-397-2740	

Information about API publications, programs and services is available on the web at www.api.org.

Product No. K78001