

Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

ANSI/API STANDARD 780
FIRST EDITION, MAY 2013

REAFFIRMED, FEBRUARY 2022



American
Petroleum
Institute



Documents

Document Sharing Hub

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.

All rights reserved. No part of this work may be reproduced, translated, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 200 Massachusetts Avenue, NW, Washington, DC 20001.

Copyright © 2013 American Petroleum Institute

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, 200 Massachusetts Avenue, NW, Washington, DC 20001. 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, 200 Massachusetts Avenue, NW, Washington, DC 20001.

Suggested revisions are invited and should be submitted to the Standards Department, API, 200 Massachusetts Avenue, NW, Washington, DC 20001, standards@api.org.

Contents

	Page
1 Scope	1
1.1 General	1
1.2 Overview	1
1.3 Sequential Activities	1
2 Normative References	2
3 Terms, Definitions, Acronyms, Abbreviations, and Symbols	2
3.1 Terms and Definitions	2
3.2 Acronyms, Abbreviations, and Symbols	9
4 Introduction to SRA Concepts	10
4.1 General	10
4.2 Security Risk Assessment and Security Management Principles	10
4.3 Risk Definition for SRA and Key Variables	11
4.4 Likelihood (<i>L</i>)	12
4.5 Consequences (<i>C</i>)	13
4.6 Threat (<i>T</i>)	14
4.7 Attractiveness (<i>A</i>)	15
4.8 Vulnerability (<i>V</i>)	15
5 SRA Approach	16
5.1 Concept and Relationship to Security Risk Management Process	16
5.2 Conducting and Reviewing the SRA	16
5.3 Validation and Prioritization of Risks	17
5.4 Risk-based Screening	17
6 SRA Approach	19
6.1 General	19
6.2 Planning for Conducting a SRA	23
6.3 SRA Team	23
6.4 SRA Objectives and Scope	24
6.5 Information Gathering, Review, and Integration	25
6.6 Sources of Information	25
6.7 Identifying Information Needs	26
6.8 Locating Required Information	26
6.9 Information Collection and Review	27
6.10 Analyzing Previous Incidents	27
6.11 Conducting a Site Inspection	27
6.12 Gathering Threat Information	27
6.13 Steps of the API SRA—Step 1: Characterization	27
6.14 Steps of the API SRA—Step 2: Threat Assessment	32
6.15 Steps of the API SRA—Step 3: Vulnerability Assessment	35
6.16 Steps of the API SRA—Step 4: Risk Analysis/Ranking	38
6.17 Steps of the API SRA—Step 5: Identify Countermeasures	40
6.18 Summary of Approach	41
6.19 Follow-up to the SRA	42

Contents

	Page
Annex A (informative) Forms and Worksheets	44
A.1 Form 1—Characterization Form	44
A.2 Form 2—Threat Assessment Form	46
A.3 Form 3—Attractiveness Form	48
A.4 Form 4—Vulnerability Analysis and Risk Assessment Form	50
A.5 Form 5—Recommendation Form	52
A.6 Alternate Form 5—Determine Residual Risk Based on Implementation of All Proposed Countermeasures	54
A.7 Optional Form 6 (if Alternate Form 5 is Used)—Proposed Countermeasure Risk Score and Priority Form	56
Annex B (informative) SRA Supporting Data Requirements	58
Annex C (informative) Examples of the SRA Process	59
C.1 Introduction	59
C.2 Examples	60
C.2.1 General	60
C.2.2 Example 1: Petroleum Distribution Terminal	61
C.2.3 Example 2: Refinery	73
C.2.4 Example 3: Pipeline	85
C.2.5 Example 4: Truck Transportation	94
C.2.6 Example 5: Rail Transportation	103
Bibliography	112
Figures	
1 Security Risk Definition	12
2 Target Attractiveness Factors	16
3 Recommended Times for Conducting and Reviewing the SRA	17
4 API Security Risk Assessment Methodology	19
5 API Security Risk Assessment Methodology—Step 1	20
6 API Security Risk Assessment Methodology—Step 2	21
7 API Security Risk Assessment Methodology—Steps 3 to 5	22
8 API SRA team Members	24
9 SRA Sample Objectives Statement	24
10 Example Risk Ranking Matrix	39
C.1 API SRA Methodology Flow Diagram	60
C.2 Example Terminal Diagram	64
C.3 Example Refinery Diagram	76
C.4 Example Pipeline Diagram	88
C.5 Example Truck Transportation Diagram	97
C.6 Example Rail Transportation Diagram	106

Contents

Page

Tables

1	Security Events of Concern	25
2	Description of Step 1 and Substeps	28
3	Example List of Candidates to be Considered as Critical Assets	29
4	Possible Consequences of SRA Security Events by Threat Agent.	30
5	Example Definitions of Consequences of the Event.	31
6	Description of Step 2 and Substeps	33
7	Threat Ranking Criteria.	34
8	Target Attractiveness Ranking Definition.	36
9	Description of Step 3 and Substeps	36
10	Layers of Countermeasures Guidance	38
11	Vulnerability Ranking Criteria	38
12	Description of Step 4 and Substeps	39
13	Description of Step 5 and Substeps	40

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.

<i>A</i>	attractiveness
<i>C</i>	consequence (initial consequence without consideration of any existing countermeasures)
<i>C₁</i>	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	<i>Code of Federal Regulations</i>
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	
$R_s = \text{a function of } (C, V, T)$	
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, $R_s = \text{a function of } (C, L_1, L_2)$ 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.

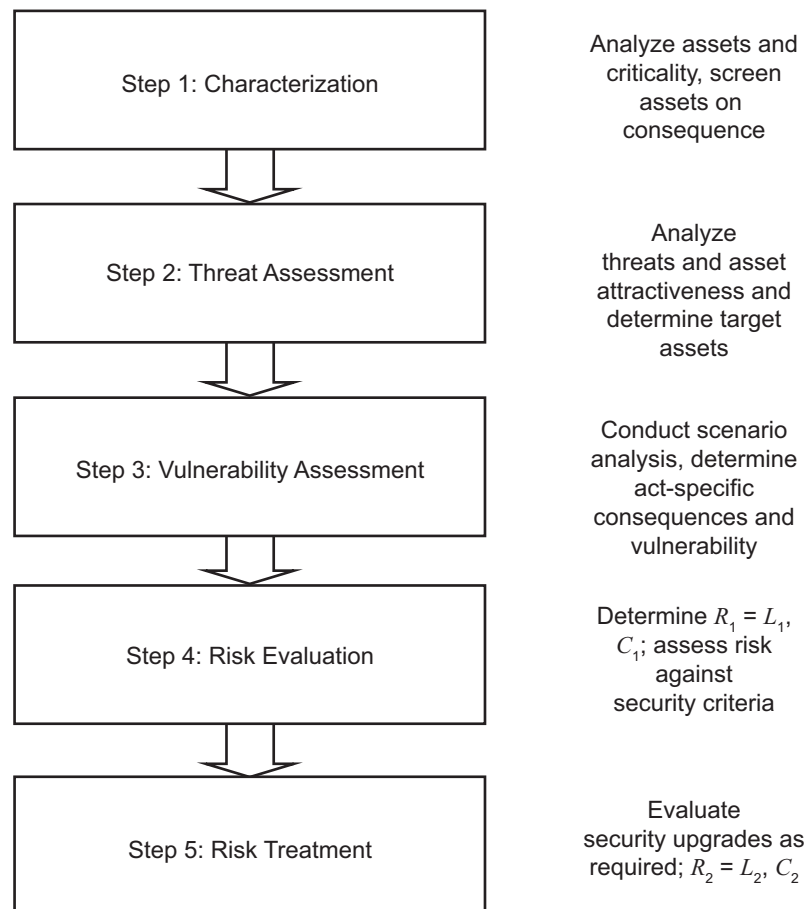


Figure 4—API Security Risk Assessment Methodology

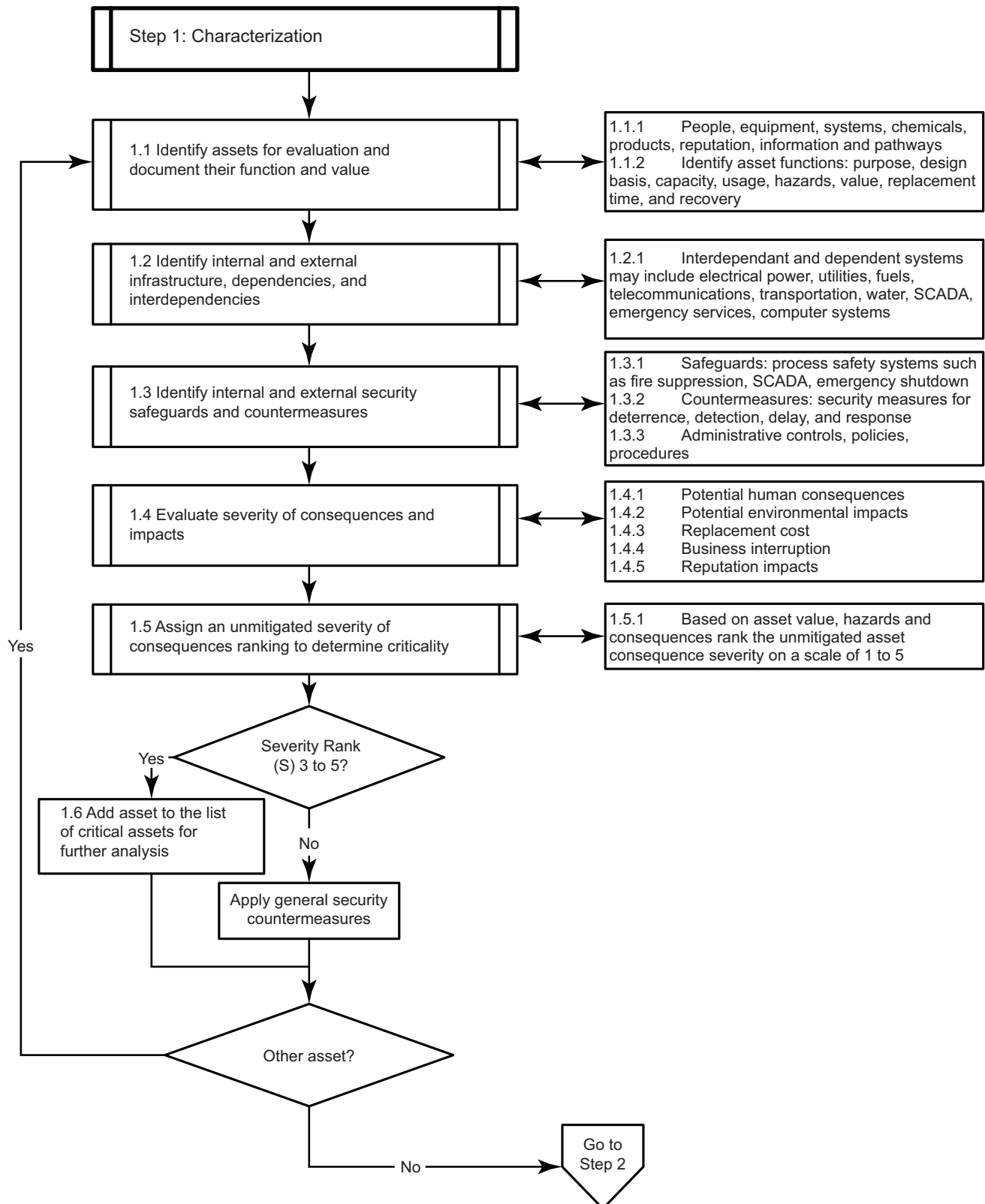


Figure 5—API Security Risk Assessment Methodology—Step 1



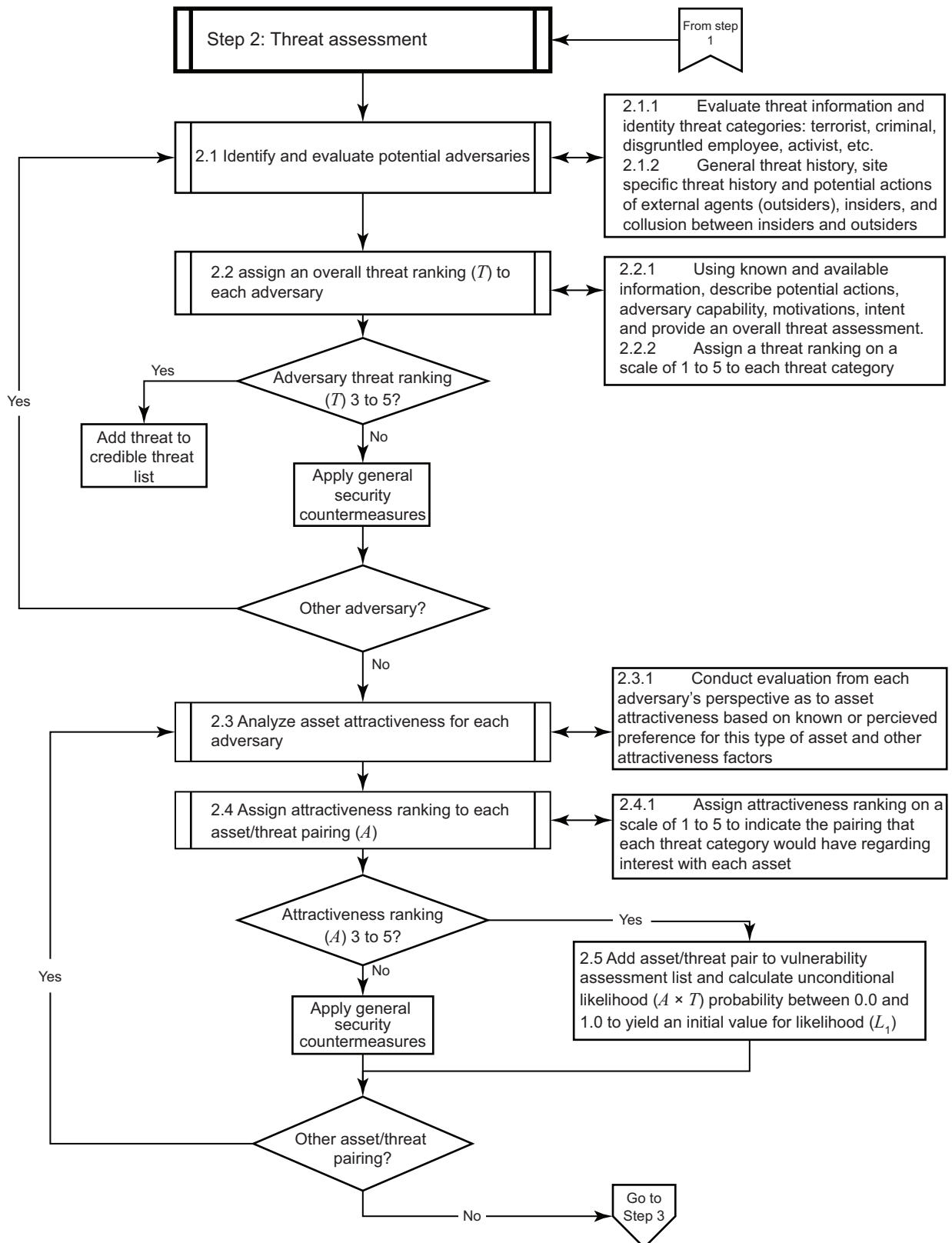


Figure 6—API Security Risk Assessment Methodology—Step 2

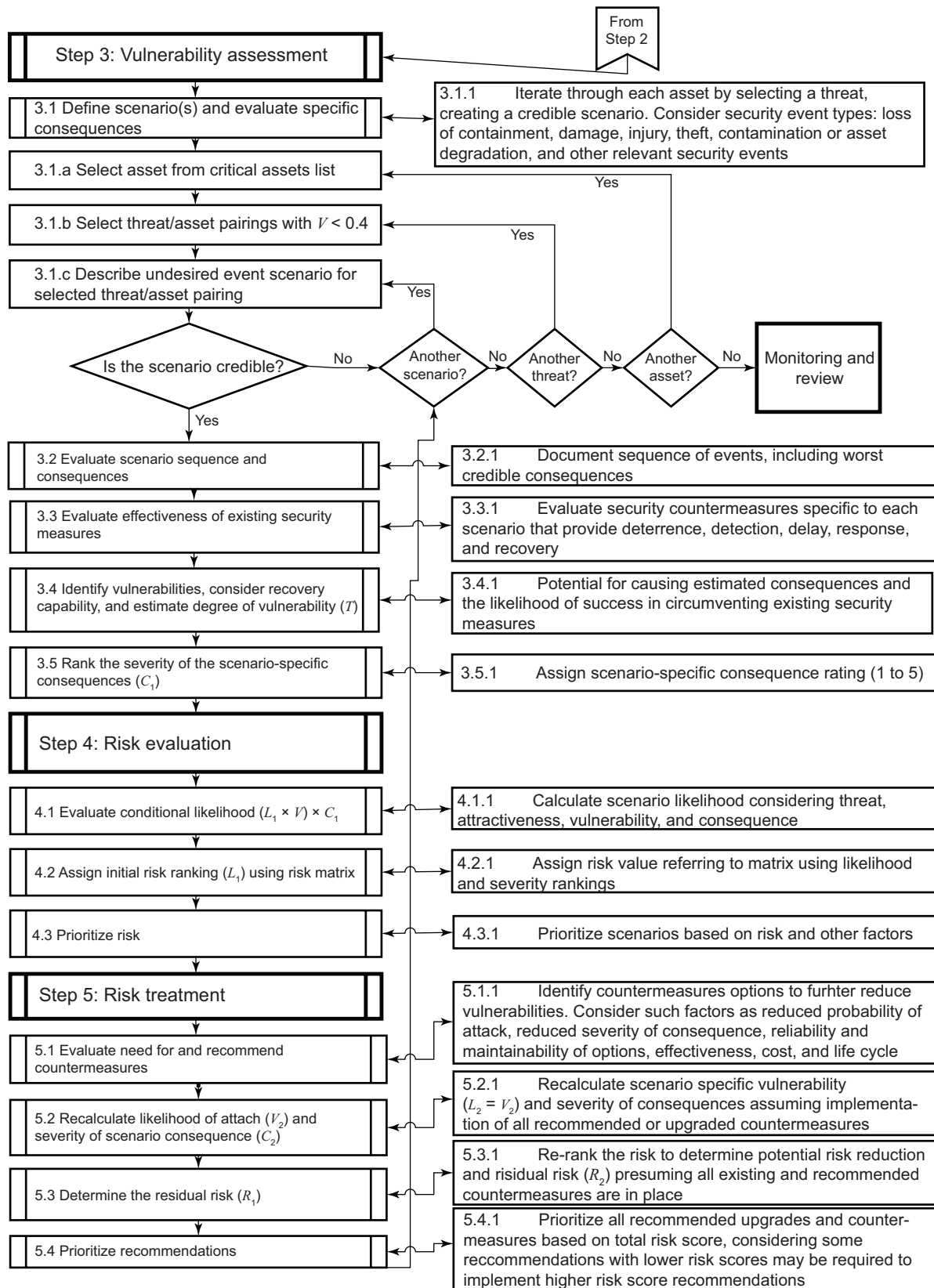


Figure 7—API Security Risk Assessment Methodology—Steps 3 to 5

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.	
—	<i>Team Leader</i> —Knowledge of and experience with the SRA methodology (not necessarily the most experienced security person).
—	<i>Security Representative</i> —Knowledge of facility security procedures, methods and systems.
—	<i>Safety Representative</i> —Knowledge of potential process hazards, process safety procedures, methods, and systems of the facility and emergency response capabilities and procedures.
—	<i>Facility Representative</i> —Knowledge of the design of the facility under study including asset value, function, criticality, and facility procedures.
—	<i>Operations Representative</i> —Knowledge of the facility process and equipment operation.
—	<i>Information Systems/Automation Representative (for Cyber Security Assessment)</i> —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.	
—	<i>Security Specialist</i> —Knowledge of threat assessment, terrorism, weapons, targeting and insurgency/guerilla warfare, or specialized knowledge of detection technologies or other available countermeasures.
—	<i>Cyber Security Specialist</i> —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.
—	<i>Process Specialist</i> —Knowledge of the process design and operations.
—	<i>Management</i> —Knowledge of business management practices, goals, budgets, plans, and other management systems.
—	<i>Human Resources</i> —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 handling 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 (<i>C</i>) 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 <i>C</i> = 3 to 5, then add asset to the critical asset list; if <i>C</i> = 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 <i>C</i> 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."