Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

ANSI/API STANDARD 780
SECOND EDITION, MAY 2026





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. The use of API publications is voluntary. In some cases, third parties or authorities having jurisdiction may choose to incorporate API standards by reference and may mandate compliance.

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 ensure 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.

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, Suite 1100, Washington, DC 20001.

Copyright © 2025 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.

The verbal forms used to express the provisions in this document are as follows.

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

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

May: As used in a standard, “may” denotes a course of action permissible within the limits of a standard.

Can: As used in a standard, “can” denotes a statement of possibility or capability.

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, Suite 1100, 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, Suite 1100, Washington, DC 20001.

Suggested revisions are invited and should be submitted to the Standards Department, API, 200 Massachusetts Avenue, NW, Suite 1100, Washington, DC 20001, standards@api.org.

Contents

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 Security Risk Assessment Concepts 10
4.1 General 10
4.2 Security Risk Assessment and Security Management Principles 10
4.3 Risk Definition for Security Risk Assessment and Key Variables 11
4.4 Likelihood (L) 12
4.5 Consequences (C) 13
4.6 Threat (T) 14
4.7 Attractiveness (A) 15
4.8 Vulnerability (V) 16

5 Security Risk Assessment Approach 17
5.1 Concept and Relationship to Security Risk Management Process 17
5.2 Conducting and Reviewing the Security Risk Assessment 17
5.3 Validation and Prioritization of Risks 17
5.4 Risk-based Screening 18

6 Security Risk Assessment Approach 19
6.1 General 19
6.2 Planning for Conducting a Security Risk Assessment 24
6.3 Security Risk Assessment Team 24
6.4 Security Risk Assessment Objectives and Scope 25
6.5 Information Gathering, Review, and Integration 26
6.6 Sources of Information 26
6.7 Identifying Information Needs 27
6.8 Locating Required Information 27
6.9 Information Collection and Review 28
6.10 Analyzing Previous Incidents 28
6.11 Conducting a Site Inspection 28
6.12 Gathering Threat Information 28
6.13 Steps of the API Security Risk Assessment—Step 1: Characterization 28
6.14 Steps of the API Security Risk Assessment—Step 2: Threat Assessment 34
6.15 Steps of the API Security Risk Assessment—Step 3: Vulnerability Assessment 37
6.16 Steps of the API Security Risk Assessment—Step 4: Risk Analysis/Ranking 40
6.17 Steps of the API Security Risk Assessment—Step 5: Identify Countermeasures 41
6.18 Summary of the Approach 42
6.19 Follow-up to the Security Risk Assessment 44

Annex A (informative) Forms and Worksheets 45
A.1 Form 1—Characterization 45
A.2 Form 2—Threat Assessment 47
A.3 Form 3—Attractiveness Assessment 49
A.4 Form 4—Vulnerability Assessment and Risk Evaluation 51
A.5 Form 5—Recommendations 53
A.6 Alternate Form 5—Recommendations: Determine Residual Risk Based on Implementation of Proposed Countermeasures 55

A.7 Optional Form 6 (if Alternate Form 5 Is Used)—Proposed Countermeasure Risk Reduction Score and Priority 57

Annex B (informative) Security Risk Assessment Supporting Data Requirements 59

Annex C (informative) Examples of the Security Risk Assessment Process 61
C.1 Introduction 61
C.2 Examples 62
C.2.1 General 62
C.2.2 Example 1: Petroleum Distribution Terminal 62
C.2.3 Example 2: Refinery 75
C.2.4 Example 3: Pipeline 88
C.2.5 Example 4: Truck Transportation 98
C.2.6 Example 5: Rail Transportation 108

Bibliography 118

Figures

1 Security Risk Definition 12
2 Target Attractiveness Factors 16
3 Recommended Times for Conducting and Reviewing the Security Risk Assessment 17
4 API Security Risk Assessment Methodology 20
5 API Security Risk Assessment Methodology—Step 1 21
6 API Security Risk Assessment Methodology—Step 2 22
7 API Security Risk Assessment Methodology—Steps 3 to 5 23
8 API Security Risk Assessment Team Members 25
9 Security Risk Assessment Sample Objectives Statement 25
10 Example Risk Ranking Matrix 41
C.1 API Security Risk Assessment Methodology Flow Diagram 62
C.2 Example Terminal Diagram 66
C.3 Example Refinery Diagram 79
C.4 Example Pipeline Diagram 92
C.5 Example Truck Transportation Diagram 101
C.6 Example Rail Transportation Diagram 111

Tables

1 Security Scenarios of Concern 26
2 Description of Step 1 and Substeps 29
3 Example List of Candidates to Be Considered as Critical Assets 30
4 Possible Consequences of Security Risk Assessment Security Events by Threat Agent 32
5 Example Definitions of Consequences of the Event 33
6 Description of Step 2 and Substeps 34
7 Threat Ranking Criteria 36
8 Target Attractiveness Ranking Definition 37
9 Description of Step 3 and Substeps 38
10 Layers of Countermeasures Guidance 39
11 Vulnerability Ranking Criteria 40
12 Description of Step 4 and Substeps 41
13 Description of Step 5 and Substeps 42

Introduction

API developed this security risk assessment (SRA) methodology as a universal approach for assessing security risk at petroleum and petrochemical facilities, as well as other related assets. The information contained herein has been developed in cooperation with the 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 may support regulatory compliance.

This standard does not change the basic methodology. The major changes include renaming the methodology from a security vulnerability analysis methodology to an SRA methodology to reflect the full scope of the analysis as a risk assessment versus a vulnerability analysis, which is only one step of the methodology. The update considered improvements based on recent developments and experiences from practical use. 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 because the five-step process is a risk assessment including characterization, threat assessment, vulnerability assessment, risk evaluation, and risk treatment steps.

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 reviewed 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 and managing risk 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 industries, 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. An SRA is a systematic process that evaluates the likelihood that a given threat factor (e.g. activist, criminal, disgruntled insider, or terrorist) will be successful in committing an intentional act (e.g. damage and 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 an 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.

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. It is important to include those with security responsibilities at the facility on the SRA team, as they can provide context to security issues and will likely have to implement any SRA recommendations.

1.3 Sequential Activities

The API SRA methodology includes the following five sequential steps.