Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries

ANSI/API STANDARD 780
FIRST EDITION, MAY 2013

AMERICAN PETROLEUM INSTITUTE

Special Notes

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

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

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

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

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

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

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

Foreword

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

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

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

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

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

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

Contents

Contents

Contents

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;