



CGA P-50—2021

STANDARD FOR SITE SECURITY

FOURTH EDITION

This document licensed for the sole use of the purchaser. It may not be shared with any other person or used after the expiration date without the express written permission of the CGA. Any unauthorized use, reproduction, distribution, or modification of this printed page will result in a \$5,000 liquidated damages fee plus loss of access to CGA publications for one year for your company.

Full document details: CGA P-50-2021

PLEASE NOTE:

The information contained in this document was obtained from sources believed to be reliable and is based on technical information and experience currently available from members of the Compressed Gas Association, Inc. and others. However, the Association or its members, jointly or severally, make no guarantee of the results and assume no liability or responsibility in connection with the information or suggestions herein contained. Moreover, it should not be assumed that every acceptable commodity grade, test or safety procedure or method, precaution, equipment or device is contained within, or that abnormal or unusual circumstances may not warrant or suggest further requirements or additional procedure.

This document is subject to periodic review, and users are cautioned to obtain the latest edition. The Association invites comments and suggestions for consideration. In connection with such review, any such comments or suggestions will be fully reviewed by the Association after giving the party, upon request, a reasonable opportunity to be heard. Proposed changes may be submitted via the Internet at our web site, www.cganet.com.

This document should not be confused with federal, state, provincial, or municipal specifications or regulations; insurance requirements; or national safety codes. While the Association recommends reference to or use of this document by government agencies and others, this document is purely voluntary and not binding unless adopted by reference in regulations.

A listing of all publications, audiovisual programs, safety and technical bulletins, and safety posters is available via the Internet at our website at www.cganet.com. For more information contact CGA at Phone: 703-788-2700, ext. 799. E-mail: customerservice@cganet.com.

Work Item 19-042
Security Committee

NOTE—Technical changes from the previous edition are underlined.

FOURTH EDITION: 2021
THIRD EDITION: 2014
SECOND EDITION: 2007
FIRST EDITION: 2005

© 2021 The Compressed Gas Association, Inc. All rights reserved.

All materials contained in this work are protected by United States and international copyright laws. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical including photocopying, recording, or any information storage and retrieval system without permission in writing from The Compressed Gas Association, Inc. All requests for permission to reproduce material from this work should be directed to The Compressed Gas Association, Inc., 8484 Westpark Drive, Suite 220, McLean, VA 22102. You may not alter or remove any trademark, copyright or other notice from this work.



Contents	Page
1 Introduction.....	1
2 Scope	1
3 Definitions.....	1
4 Resource information	4
5 Facility security tier ranking	5
6 Security vulnerability assessment	5
6.1 Project planning.....	6
6.2 Facility characterization.....	7
6.3 Threat assessment.....	10
6.4 Vulnerability analysis.....	10
6.5 Countermeasure identification.....	11
6.6 Third-party validation.....	12
7 Physical security.....	12
7.1 General information	12
7.2 Signage	13
7.3 Perimeter barrier.....	13
7.4 Perimeter clearance	15
7.5 Bollards.....	15
7.6 Access control	15
7.7 Lighting.....	17
7.8 High risk security chemicals storage	17
7.9 Loss prevention and material control/accountability.....	17
7.10 Control room and systems security	18
7.11 Policies and procedures	18
7.12 Information (cyber) security.....	19
7.13 Intelligence	19
7.14 Incidents	20
7.15 Reporting	20
7.16 Investigation	20
7.17 Analysis	20
8 Management of change.....	20
9 National Terrorism Advisory System	20
10 Crisis management plans and emergency response plans.....	21
11 Employee and contractor security issues.....	21
12 Periodic assessment and audit	21
13 References	22
14 Additional information.....	22
Tables	
Table 1—Tier ranking.....	5
Table 2—Minimum physical security layers of protection	14
Figures	
Figure 1—Security vulnerability assessment management process.....	6
Figure 2—Layers of protection	10
Appendix	
Appendix A—Site security training and awareness frequency (Informative)	23

1 Introduction

Implementation of security measures are a part of the industrial gas industry culture that protect facilities, employees, and the community by reducing the risk of a wide range of threats and mitigating the effects of incidents such as vandalism, sabotage, workplace violence, and terrorism. Security measures enhance process safety management (PSM), risk management programs (RMP), worker safety, and environmental protection.

A security program should include the following elements:

- site screening for risk prioritization;
- security vulnerability assessment (SVA);
- incident reporting and investigation;
- emergency response and crisis management;
- employee and contractor security issues;
- periodic reassessment; and
- employee security awareness training.

The Compressed Gas Association (CGA) thanks the Center for Chemical Process Safety (CCPS) of the American Institute of Chemical Engineers for granting permission to reproduce and adapt large sections of its book *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites* [1].¹

2 Scope

This publication provides instruction to the industrial gas industry for assessing security risks and identifying and implementing preventive security measures at fixed sites. It is intended as a resource to help managers at individual facilities make security decisions based on risk.

The publication does not attempt to provide an all-inclusive list of security considerations for industrial gas companies nor does it address transportation security and security at customer sites. Additional security information is contained in CGA P-51, *Standard for Transportation Security in the Compressed Gas Industry* and CGA P-52, *Security Guidelines for Qualifying Customers Purchasing Compressed Gases* [2, 3].

3 Definitions

For the purpose of this publication, the following definitions apply.

3.1 Publication terminology

3.1.1 Shall

Indicates that the procedure is mandatory. It is used wherever the criterion for conformance to specific recommendations allows no deviation.

3.1.2 Should

Indicates that a procedure is recommended.

3.1.3 May

Indicates that the procedure is optional.

3.1.4 Will

Is used only to indicate the future, not a degree of requirement.

¹ References are shown by bracketed numbers and are listed in order of appearance in the reference section.

3.1.5 Can

Indicates a possibility or ability.

3.2 Technical definitions**3.2.1 Adversary**

Individual, group, organization, or government that conducts activities or has the intention and capability to conduct activities detrimental to critical assets.

NOTE—Adversaries can include foreign intelligence services, political and terrorist groups, criminals, rogue employees, and private interests. Adversaries can also include site insiders, site outsiders, or the two acting in collusion.

3.2.2 Asset

Person, environment, facility, material, information, business reputation, or activity that has a positive value to a business.

NOTE—An asset can have value to an adversary as well as a business, although the nature and magnitude of those values can differ. Assets included in a security vulnerability assessment include the community and the environment surrounding a site.

3.2.3 High risk security chemicals (HRSC)

Chemical that is a likely target for terrorist or criminal activity.

NOTE—Formerly referred to as chemical of concern (COC)/chemical of interest (COI)).

NOTE—The chemical can be one that is regulated or one that is of concern to the compressed gas industry, such as nitrous oxide.

3.2.4 Consequence

Amount of loss or damage expected from a successful attack against an asset.

NOTE—Loss can be monetary but can also include political, morale, operational, or other impacts. Some examples of relevant consequences in a SVA include injury or death; significant disruption to public, private, or company operations; environmental damage; financial loss; loss of critical data; and loss of reputation.

3.2.5 Countermeasure

Action taken or physical capability provided to reduce or eliminate vulnerabilities.

3.2.6 Cyber security

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

3.2.7 Delay

Countermeasure strategy that provides various barriers to slow the progress of an adversary's attempt to penetrate a site.

NOTE—A delay strategy is intended to prevent theft or attack.

3.2.8 Drug Enforcement Administration (DEA)

United States agency that controls the manufacture, sale, and distribution of specified drugs and the chemicals that are considered precursors to those drugs.

3.2.9 Detect

Countermeasure strategy that identifies an adversary attempting to commit or in the process of committing a terrorist or criminal activity.

NOTE—Detection includes real-time observation, post-incident analysis, and identification of the adversary.

3.2.10 Deter

Countermeasure strategy that prevents or discourages a breach of security by causing fear or doubt.

NOTE—Physical security deterrence includes warning signs, lights, uniformed guards, cameras, and barriers.

3.2.11 Intelligence

Information that characterizes specific or general threats including the motivation, capabilities, and activities of adversaries.

3.2.12 Intent

Course of action that an adversary intends to follow.

3.2.13 Layers of protection

Multiple independent, overlapping layers of security.

NOTE—Layers of protection can include counter surveillance, counter intelligence, physical security, and cyber security (concentric rings of protection).

3.2.14 Mitigation

Action that causes a consequence to be less severe.

3.2.15 Physical security

Security systems and architectural features that increase protection.

NOTE—Examples include fencing, doors, gates, walls, turnstiles, locks, vehicle barriers, and hardened glass.

3.2.16 Risk

Potential for damage to or loss of an asset.

NOTE—Risk in the context of chemical process security is the potential for a catastrophic outcome. Examples include intentional release of hazardous materials to the atmosphere, theft of chemicals that can be used as weapons or for other criminal activities, contamination of chemicals that can later harm the public, or economic costs of the damage or disruption of a chemical process.

3.2.17 Security risk assessment

Process of predicting the likelihood that an adversary will successfully exploit a company's vulnerability as well as predicting the resulting consequences.

NOTE—A security risk assessment provides the basis for rank ordering risks to establish priorities for the application of countermeasures.

3.2.18 Security plan

Document describing a plan that addresses security issues and related events including security assessment and mitigation options.

NOTE—A security plan includes security alert levels and response measures.

3.2.19 Security vulnerability assessment (SVA)

Evaluation of the possibility of an adversary successfully exploiting a company's vulnerability and the degree of damage or impact that can result.

NOTE—SVAs are not a quantitative risk analysis; they are qualitative, using the best judgment of security and safety professionals. The determination of risk (qualitatively) is the desired outcome of the SVA. It provides the basis for rank ordering the security-related risks to establish priorities for the application of countermeasures.

3.2.20 Target attractiveness

Estimate of the value of a target to an adversary.

3.2.21 Technical security

Electronic systems for increased protection (or for other security purposes).

NOTE—Technical security can include access control systems, card readers, keypads, electric locks, remote control openers, alarm systems, intrusion detection equipment, motion detectors, annunciating and reporting systems, central stations monitoring, video surveillance equipment, voice communications systems, listening devices, computer security, encryption, data auditing, and scanners.

3.2.22 Terrorism

Unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, to promote political or social objectives.

3.2.23 Threat

Indication, circumstance, or event that can cause loss of or damage to an asset, or the intention and capability of an adversary to cause loss of or damage to an asset.

3.2.24 Vulnerabilities

Weakness that can be exploited by an adversary to gain access to an asset.

NOTE—Vulnerabilities can include but are not limited to building characteristics, equipment properties, personnel practices and behaviors, locations of people, equipment, and buildings, or operational and personnel practices.

4 Resource information

This publication was developed using resource material from CCPS and the American Chemistry Council (ACC). The ACC *Responsible Care Security Code* is a helpful reference for companies seeking information in the following areas:

- security risk assessment and prevention strategies;
- security policies;
- collaboration with other corporate departments and with local, state, and national law enforcement agencies, local emergency planning committees, etc.;
- incident reporting systems;
- employee training and security awareness;
- incident investigations;
- emergency response and crisis management;
- periodic reassessment of the security plan for physical security including access control, perimeter protection, intrusion detection, security officers, ongoing testing and maintenance, and backup systems;
- employee security measures including prudent hiring and termination practices;
- workplace violence prevention and response; and
- information, computer, and network security [4].

The ACC *Responsible Care Security Code* and other reference documents are available at the ACC public website.

5 Facility security tier ranking

Facility security ranking is divided into four levels (Tiers 1-4). Tier 1 is the highest level of concern.

Tier rankings are determined by the classification and quantity of high risk security chemicals (HRSC) present at a site in addition to consideration of the following risk factors:

- intentional equipment damage or malicious release with loss of containment of hazardous chemicals resulting in multiple casualties, severe site damage, and significant public or environmental impact;
- chemical theft with the intent to cause severe harm at the facility or off site, or the intent to use the chemical for illegal activity; and
- contamination of product that causes harm to workers or to the public at the facility or off site.

Short term storage (less than 48 hours) for items in transport does not affect the overall tier ranking of a facility. See 7.8 for additional information.

Table 1 contains the HRSC and quantities that determine tier ranking.

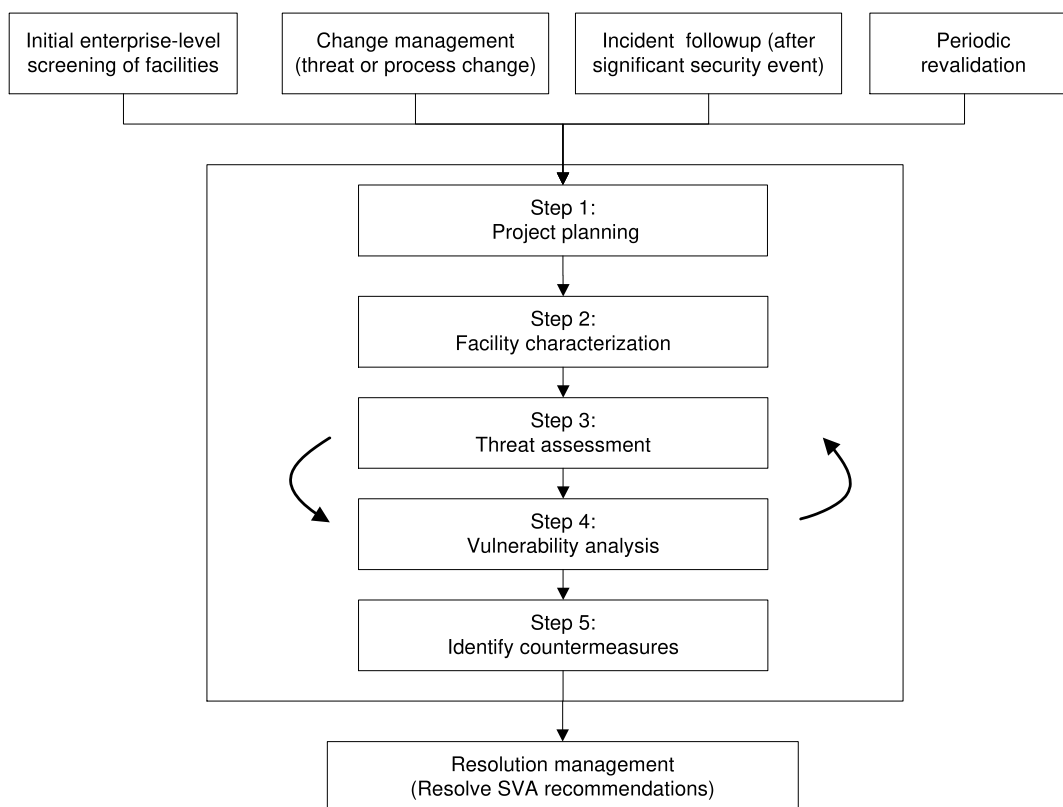
Table 1—Tier ranking

Rank	High risk security chemicals	Quantity
Tier 1	• Toxic, 2.3, hazard zone A with the exception of chlorine • Toxic, 2.3, hazard zone B with the exception of chlorine	Any quantity
Tier 2	• Toxic, 2.3, hazard zone C and chlorine • Toxic, 2.3, hazard zone D and chlorine • DEA	Cylinders > 2 000 lb Bulk > 15 000 lb
	Flammable bulk	> 100 000 lb
Tier 3	• Toxic, 2.3, hazard zone C and chlorine • Toxic, 2.3, hazard zone D and chlorine • DEA	Cylinders < 2 000 lb Bulk < 15 000 lb
	Flammable bulk	10 000 lb to 100 000 lb
	Oxygen bulk	> 250 000 gal
Tier 4	Nitrous oxide (cylinders or bulk)	Any quantity
	Flammable bulk	< 10 000 lb
	Oxygen bulk	< 250 000 gal

6 Security vulnerability assessment

The SVA is used to determine which assets require protection, the threats that can be posed against those assets, and the likelihood and consequences of attacks against those assets. The SVA is intended to: identify security hazards, threats, and vulnerabilities facing a fixed facility handling hazardous materials and unattended facilities; to protect the facility from malicious acts; and to evaluate the countermeasures to ensure the protection of the public, personnel, national interests, the environment, and the company. Figure 1 depicts a flow chart for the SVA management process.

There are a number of methodologies available for conducting an SVA. At the request of the ACC, CCPS developed an SVA methodology and established a set of criteria to define minimum acceptable standards for an SVA. See Section 12 for information on the websites where CCPS and other SVA methodologies are available.



NOTE—Copyright® (2002) by the Center for Chemical Process Safety of the American Institute of Chemical Engineers (www.aiche.org/ccps) and reproduced with permission of AIChE.

Figure 1—Security vulnerability assessment management process

6.1 Project planning

SVA planning includes: selecting a multidisciplinary team skilled in security and process safety to conduct the analysis, determining the objectives and scope, and developing a plan to address the individual sites based on the initial screening that was performed.

6.1.1 Team selection

An SVA team typically consists of cross-functional subject matter experts (SME). The size of the team is determined taking into consideration the facility complexity, hazards present, and expertise of the team members. One person should serve as the team leader. The team should have skills in security, process safety, and plant operations including SVA methodology, process safety analysis, and security procedures, methods, and systems.

6.1.2 Objectives

Defining objectives helps focus the SVA effort on issues that are of vital interest to the employees, the company, the industry, and the public. A key consideration should be the protection of the public from a terrorist or criminal event using chemicals obtained or released on site or off site.

6.1.3 Scope

The SVA team determines which facilities and threats (security event types) a company wants to address in the SVA process.