

Security management for petroleum and natural gas industry systems



Currently in preview, click buy full version

Legal Notice for Standards

Canadian Standards Association (CSA) standards are developed through a consensus standards development process approved by the Standards Council of Canada. This process brings together volunteers representing varied viewpoints and interests to achieve consensus and develop a standard. Although CSA administers the process and establishes rules to promote fairness in achieving consensus, it does not independently test, evaluate, or verify the content of standards.

Disclaimer and exclusion of liability

This document is provided without any representations, warranties, or conditions of any kind, express or implied, including, without limitation, implied warranties or conditions concerning this document's fitness for a particular purpose or use, its merchantability, or its non-infringement of any third party's intellectual property rights. CSA does not warrant the accuracy, completeness, or currency of any of the information published in this document. CSA makes no representations or warranties regarding this document's compliance with any applicable statute, rule, or regulation.

IN NO EVENT SHALL CSA, ITS VOLUNTEERS, MEMBERS, SUBSIDIARIES, OR AFFILIATED COMPANIES, OR THEIR EMPLOYEES, DIRECTORS, OR OFFICERS, BE LIABLE FOR ANY DIRECT, INDIRECT, OR INCIDENTAL DAMAGES, INJURY, LOSS, COSTS, OR EXPENSES, HOWSOEVER CAUSED, INCLUDING BUT NOT LIMITED TO SPECIAL OR CONSEQUENTIAL DAMAGES, LOST REVENUE, BUSINESS INTERRUPTION, LOST OR DAMAGED DATA, OR ANY OTHER COMMERCIAL OR ECONOMIC LOSS, WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR ANY OTHER THEORY OF LIABILITY, ARISING OUT OF OR RESULTING FROM ACCESS TO OR POSSESSION OR USE OF THIS DOCUMENT, EVEN IF CSA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INJURY, LOSS, COSTS, OR EXPENSES.

In publishing and making this document available, CSA is not undertaking to render professional or other services for or on behalf of any person or entity or to perform any duty owed by any person or entity to another person or entity. The information in this document is directed to those who have the appropriate degree of experience to use and apply its contents, and CSA accepts no responsibility whatsoever arising in any way from any and all use of or reliance on the information contained in this document.

CSA is a private not-for-profit company that publishes voluntary standards and related documents. CSA has no power, nor does it undertake, to enforce compliance with the contents of the standards or other documents it publishes.

Intellectual property rights and ownership

As between CSA and the users of this document (whether it be in printed or electronic form), CSA is the owner, or the authorized licensee, of all works contained herein that are protected by copyright, all trade-marks (except as otherwise noted to the contrary), and all inventions and trade secrets that may be contained in this document, whether or not such inventions and trade secrets are protected by patents and applications for patents. Without limitation, the unauthorized use, modification, copying, or disclosure of this document may violate laws that protect CSA's and/or others' intellectual property and may give rise to a right in CSA and/or others to seek legal redress for such use, modification, copying, or disclosure. To the extent permitted by licence or by law, CSA reserves all intellectual property rights in this document.

Patent rights

Attention is drawn to the possibility that some of the elements of this standard may be the subject of patent rights. CSA shall not be held responsible for identifying any or all such patent rights. Users of this standard are expressly advised that determination of the validity of any such patent rights is entirely their own responsibility.

Authorized use of this document

This document is being provided by CSA for informational and non-commercial use only. The user of this document is authorized to do only the following:

If this document is in electronic form:

- load this document onto a computer for the sole purpose of reviewing it;
- search and browse this document; and
- print this document if it is in PDF format.

Limited copies of this document in print or paper form may be distributed only to persons who are authorized by CSA to have such copies, and only if this Legal Notice appears on each such copy.

In addition, users may not and may not permit others to

- alter this document in any way or remove this Legal Notice from the attached standard;
- sell this document without authorization from CSA; or
- make an electronic copy of this document.

If you do not agree with any of the terms and conditions contained in this Legal Notice, you may not load or use this document or make any copies of the contents hereof, and if you do make such copies, you are required to destroy them immediately. Use of this document constitutes your acceptance of the terms and conditions of this Legal Notice.



CANADIAN STANDARDS
ASSOCIATION

CSA Standards Update Service

Z246.1-09

August 2009

Title: *Security management for petroleum and natural gas industry systems*

Pagination: **29 pages** (viii preliminary and 21 text), each dated **August 2009**

Automatic notifications about any updates to this publication are available.

- To register for e-mail notifications, and/or to download any existing updates in PDF, enter the Online Store at **www.ShopCSA.ca** and click on **My Account** on the navigation bar.

The **List ID** for this document is **2020275**.

- To receive printed updates, please complete and return the attached card.



Name _____

Organization _____

Address _____

City _____

Province/State _____

Country _____ Postal/Zip Code _____

E-mail _____

I consent to CSA collecting and using the above information to send me updates relating to this publication.

Visit CSA's policy on privacy at www.csagroup.org/legal to find out how we protect your personal information.

Z246.1-09

Currently in preview, click buy full version

**ASSOCIATION CANADIENNE DE
NORMALISATION**

BUREAU CENTRAL DE L'INFORMATION
5060, SPECTRUM WAY, BUREAU 100
MISSISSAUGA ON L4W 5N6
CANADA

**CANADIAN STANDARDS
ASSOCIATION**

CONSOLIDATED MAILING LIST
5060 SPECTRUM WAY, SUITE 100
MISSISSAUGA ON L4W 5N6
CANADA

Affranchir suffisamment
Place Stamp Here

CSA Standard

Z246.1-09

***Security management for petroleum and
natural gas industry systems***



**CANADIAN STANDARDS
ASSOCIATION**

®Registered trade-mark of Canadian Standards Association

*Published in August 2009 by Canadian Standards Association
A not-for-profit private sector organization
5060 Spectrum Way, Suite 100, Mississauga, Ontario, Canada L4W 5N6
1-800-463-6727 • 416-747-4044*

Visit our Online Store at www.ShopCSA.ca



The Canadian Standards Association (CSA) prints its publications on Rolland Enviro100, which contains 100% recycled post-consumer fibre, is EcoLogo and Processed Chlorine Free certified, and was manufactured using biogas energy.

To purchase CSA Standards and related publications, visit CSA's Online Store at www.ShopCSA.ca or call toll free 1-800-463-6727 or 416-747-4044.

ISSN 1978-1-55491-281-0

Technical Editor: Laura Pelan

© Canadian Standards Association — 2009

All rights reserved. No part of this publication may be reproduced in any form whatsoever without the prior permission of the publisher.

Contents

Technical Committee on Security Management for Petroleum and Natural Gas Industry Systems vi

Preface viii

0 Introduction 1

1 Scope 2

2 Reference publications 5

3 Definitions 6

4 Security management program (SMP) 8

- 4.1 Governance 8
 - 4.1.1 General 8
 - 4.1.2 Accountability 8
- 4.2 Implementation 8
- 4.3 Competence 8
- 4.4 External practices 8
- 4.5 Internal practices 8

5 Security risk management 9

- 5.1 General 9
- 5.2 Asset characterization 10
 - 5.2.1 General 10
 - 5.2.2 Procedures 11
- 5.3 Threat assessment 11
 - 5.3.1 General 11
 - 5.3.2 Procedures 11
- 5.4 Vulnerability assessment 11
- 5.5 Risk assessment 12
- 5.6 Risk mitigation 12
- 5.7 Communication and recommendations 12

6 Information security management 13

- 6.1 General 13
- 6.2 Policies and procedures 13
- 6.3 Training and awareness 13
- 6.4 Classifying information 13
- 6.5 Handling and storage 13
- 6.6 External information 14
 - 6.6.1 General 14
 - 6.6.2 Security clearance 14
- 6.7 Records and documentation 14
- 6.8 Destruction 14

7 Information technology/control systems security 14

- 7.1 Information technology 14
- 7.2 Control systems security 14

8 Personnel security 15

- 8.1 General 15
- 8.2 Protection of personnel 15
- 8.3 Security training and awareness 15
 - 8.3.1 General 15
 - 8.3.2 Process 15
- 8.4 Employee/on-site personnel screening 16
- 8.5 Employee/on-site personnel termination 16
- 8.6 Employee travel 16

9 Physical security measures 16

- 9.1 General 16
- 9.2 Facility design and construction 16
- 9.3 Physical security 16
 - 9.3.1 General 16
 - 9.3.2 Fencing or exterior walls 16
 - 9.3.3 Signage 16
 - 9.3.4 Gates 17
 - 9.3.5 Intrusion detection systems/alarm systems 17
 - 9.3.6 Lighting 17
 - 9.3.7 Access control 17
 - 9.3.8 Locks and key control 17
 - 9.3.9 Closed circuit video (CCV) surveillance 17
 - 9.3.10 Uniformed security officers 17
 - 9.3.11 Protection of critical assets, equipment, tools, information, communication technologies (ICT), and supplies 18
 - 9.3.12 Protection of critical utilities 18

10 Security incident management 18

- 10.1 General 18
- 10.2 Process/planning 18
- 10.3 Incident documentation 19
- 10.4 Incident response 19
 - 10.4.1 General 19
 - 10.4.2 Incident reporting 19
 - 10.4.3 Security incident response 19
 - 10.4.4 Communication 19
- 10.5 Investigations 19
- 10.6 Security exercises and drills 19

11 Change management process 19

- 11.1 General 19
- 11.2 Process 20
- 11.3 Structure 20

12 Evaluation/review 20

- 12.1 General 20
- 12.2 Review 20
 - 12.2.1 General 20
 - 12.2.2 Review frequency 20
 - 12.2.3 Review input 21
 - 12.2.4 Review output 21
- 12.3 Control of nonconformance 21
- 12.4 Records 21

13 Continual improvement 21

13.1 General 21

13.2 Process 21

Figures

- 1** — Security management program overview 2
- 2** — Scope diagram — Petroleum industry systems 4
- 3** — Scope diagram — Natural gas industry systems 5
- 4** — Security risk management process 9

Technical Committee on Security Management for Petroleum and Natural Gas Industry Systems

J. Kereliuk	National Energy Board, Calgary, Alberta	<i>Chair</i>
R. Caesar	Ministry of Energy, Mines & Petroleum Resources, Victoria, British Columbia	<i>Vice-Chair</i>
A. Johnson	Enbridge Inc., Ottawa, Ontario	<i>Vice-Chair</i>
J. Anderson	CC Technologies, a DNV company, Calgary, Alberta	
N. Berry	Terasen Gas Inc., Surrey, British Columbia	
W. Bishop	Enbridge Gas Distribution, Toronto, Ontario	<i>Associate</i>
Y. Dubeau	Montréal, Québec	
G. Fotheringham	Shell Canada Limited, Calgary, Alberta	
J. Fox	US Department of Homeland Security, Arlington, Virginia, USA	
C. Galenzoski	Grant Thornton LLP, Calgary, Alberta	
D. Huot	Alberta Solicitor General & Public Security, Edmonton, Alberta	
W. Isaacs	Union Gas Limited, Chatham, Ontario	
L. Jansen	Energy Resources Conservation Board, Calgary, Alberta	
S. Kashva	Shell Canada Limited, Calgary, Alberta	<i>Associate</i>
M. Lamond	Spectra Energy, Fort St. John, British Columbia	
G. Malboeuf	Gaz Métro Inc., Montréal, Québec	<i>Associate</i>

D. Ray	Grant Thornton LLP, Calgary, Alberta	<i>Associate</i>
D. Redman	Morinville, Alberta	
Z. Saad	Canadian Energy Pipeline Association (CEPA), Calgary, Alberta	
S. Savoie	Savoie Security Associates, Ottawa, Ontario	
S. Senger	Calgary, Alberta	<i>Associate</i>
J. Sharp	US Department of Homeland Security, Arlington, Virginia, USA	<i>Associate</i>
V. Simpson	Public Safety Canada, Winnipeg, Manitoba	
B. Smith	Pembina Pipeline Corporation, Calgary, Alberta	
M. Stebner	Alliance Pipeline Ltd., Calgary, Alberta	
M. Toews	Tocra Inc., Calgary, Alberta	
L. Pelan	Canadian Standards Association, Mississauga, Ontario	<i>Project Manager</i>

Preface

This is the first edition of CSA Z246.1, *Security management for petroleum and natural gas industry systems*.

This Standard uses the concept of a security management program, and in particular risk management, to address security issues. This Standard provides a performance-based approach for use by the operator to establish governance, conduct planning, implement security operations (including detection and mitigation practices), and refine the security management program through change management and audit processes. This approach allows users to apply this Standard across the petroleum and natural gas industry.

This Standard is one of several security risk management tools. Operators need to work with other industries, as well as governmental agencies, in order to effectively manage the security of their energy infrastructure. A security management program should complement existing programs and should consider the risks and criticality of the assets being protected. Therefore, this Standard should be read in conjunction with other security legislation, safety legislation, best practices, policies, standards, and applicable codes (e.g., CSA Z662, CAN/CSA-Z731, and CSA Z1600).

CSA acknowledges that the development of this Standard was made possible, in part, by the financial support of Natural Resources Canada (NRCan).

This Standard was prepared by the Technical Committee on Security Management for Petroleum and Natural Gas Industry Systems, under the jurisdiction of the Strategic Steering Committee on Petroleum and Natural Gas Industry Systems, and has been formally approved by the Technical Committee. It will be submitted to the Standards Council of Canada for approval as a National Standard of Canada.

August 2009

Notes:

- (1) Use of the singular does not exclude the plural (and vice versa) when the sense allows.
- (2) Although the intended primary application of this Standard is stated in its Scope, it is important to note that it remains the responsibility of the users of the Standard to judge its suitability for their particular purpose.
- (3) This publication was developed by consensus, which is defined by CSA Policy governing standardization — Code of good practice for standardization as “substantial agreement. Consensus implies much more than a simple majority, but not necessarily unanimity”. It is consistent with this definition that a member may be included in the Technical Committee list and yet not be in full agreement with all clauses of this publication.
- (4) CSA Standards are subject to periodic review, and suggestions for their improvement will be referred to the appropriate committee.
- (5) All enquiries regarding this Standard, including requests for interpretation, should be addressed to Canadian Standards Association, 5060 Spectrum Way, Suite 100, Mississauga, Ontario, Canada L4W 5N6.
Requests for interpretation should
 - (a) define the problem, making reference to the specific clause, and, where appropriate, include an illustrative sketch;
 - (b) provide an explanation of circumstances surrounding the actual field condition; and
 - (c) be phrased where possible to permit a specific “yes” or “no” answer.

Committee interpretations are processed in accordance with the CSA Directives and guidelines governing standardization and are published in CSA's periodical Info Update, which is available on the CSA Web site at www.csa.ca.

Z246.1-09

Security management for petroleum and natural gas industry systems

0 Introduction

Canadians recognize the importance of a safe, secure, and reliable energy supply and that any prolonged interruption in the supply of energy, such as petroleum or natural gas, would harm the economy. Because energy infrastructure assets and systems are geographically dispersed and the operation of the infrastructure is typically managed by several different operating companies using a variety of delivery mechanisms, protecting the energy supply presents a unique challenge. In order to help petroleum and natural gas companies evaluate and respond appropriately to security threats, the Canadian Standards Association has worked with security professionals to prepare this Standard.

This Standard is based on the premise that security risks should be managed using risk-based and performance-based management processes. The foundation of a security management program is the identification and analysis of security risks on a continuing basis and the mitigation of these risks with adequate security countermeasures. The security risk management process can be used to help accomplish this task and to help the operator make decisions regarding the need for security measures. Potential threats and appropriate security measures vary based on size, location, facility type, and existing security measures. This Standard provides a means of identifying, analyzing, and reducing risks through a security risk management process. This Standard also identifies specific security risk reduction measures to be implemented. A risk-based approach recognizes that there is no uniform security management program that would apply to the entire petroleum and natural gas industry and that resources are best applied to mitigate high-risk situations. Not all security risks can be completely prevented.

A governance framework for a security management program begins with an awareness of what the program serves to protect. Effective governance ensures the protection of the key program components: people, the environment, assets, and economic stability.

An effective security management program (as illustrated in [Figure 1](#)) requires sustainable governance in the form of

- (a) legislative and policy framework;
- (b) organizational and strategic leadership;
- (c) accountability (both internal and external); and
- (d) compliance.

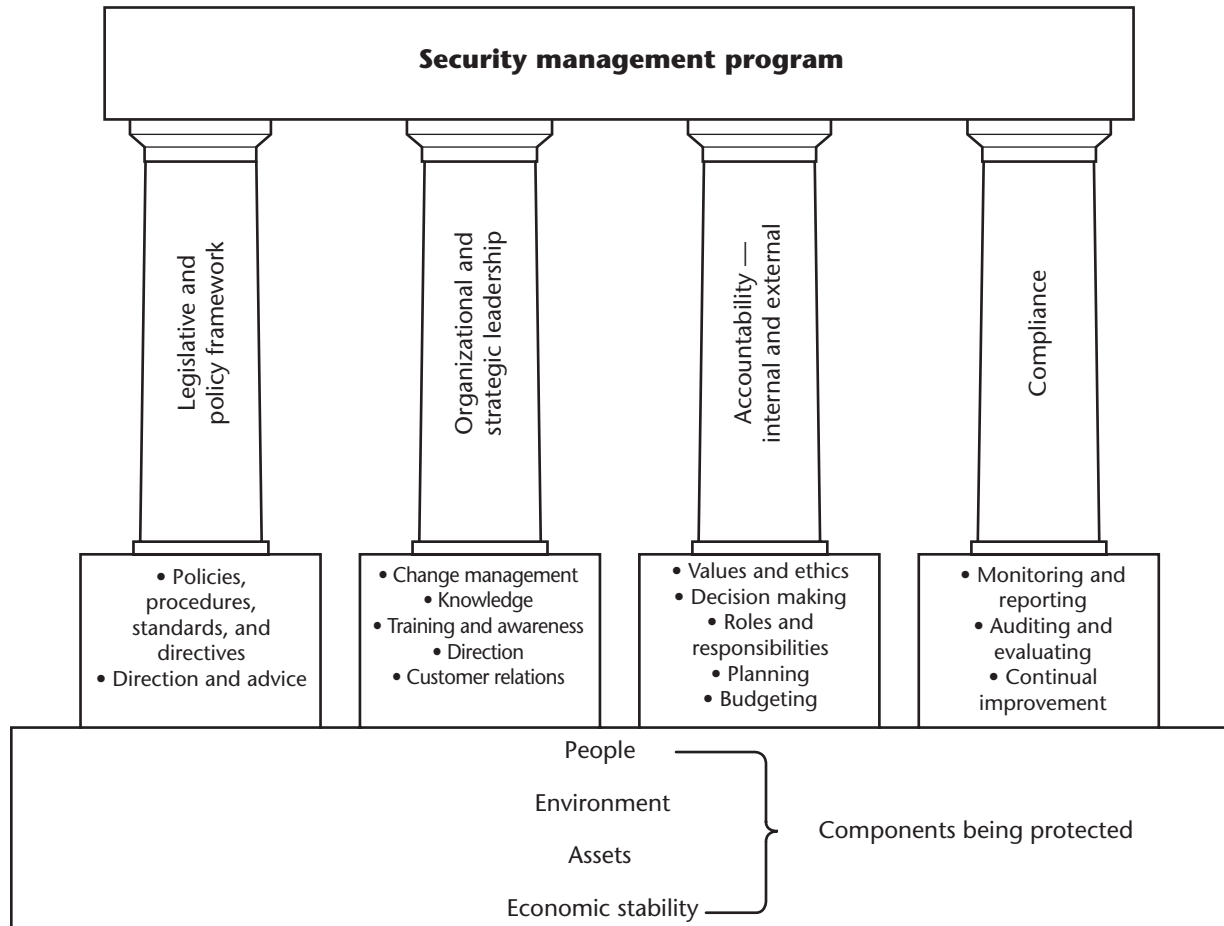


Figure 1
Security management program overview
 (See [Clause 0](#).)

1 Scope

1.1

This Standard specifies criteria for establishing a security management program for petroleum and natural gas industry systems to ensure security threats and associated risks are identified and managed. This Standard provides mitigation and response processes and procedures to prevent and minimize the impact of security incidents that could adversely affect people, the environment, assets, and economic stability.

1.2

This Standard applies to all petroleum and natural gas industry systems (as illustrated in [Figures 2 and 3](#)), including

- (a) pipeline systems handling
 - (i) oil;
 - (ii) gas;
 - (iii) oil-field water;
 - (iv) liquid products;

- (v) multi-phase fluids;
- (vi) slurries; and
- (vii) system supports, including
 - (1) meter stations;
 - (2) compressor stations;
 - (3) pump stations;
 - (4) tank farms;
 - (5) terminals; and
 - (6) all assets that support Items (1) to (5);
- (b) liquefied natural gas (LNG) production, storage, and handling facilities;
- (c) storage of hydrocarbons in underground formations;
- (d) petrochemical installations, including
 - (i) refineries;
 - (ii) gas processing plants;
 - (iii) liquefied petroleum gas plants;
 - (iv) synthetic natural gas plants; and
 - (v) coal gasification plants; and
- (e) oil and gas production, treatment, processing, and storage operations not covered in Items (a) to (d).

1.3

This Standard does not apply to offshore petroleum and natural gas platforms.

1.4

The requirements of this Standard are applicable to all operators, regardless of the size or number of their assets.

1.5

In CSA Standards, “shall” is used to express a requirement, i.e., a provision that the user is obliged to satisfy in order to comply with the standard; “should” is used to express a recommendation or that which is advised but not required; “may” is used to express an option or that which is permissible within the limits of the standard; and “can” is used to express possibility or capability. Notes accompanying clauses do not include requirements or alternative requirements; the purpose of a note accompanying a clause is to separate from the text explanatory or informative material. Notes to tables and figures are considered part of the table or figure and may be written as requirements. Annexes are designated normative (mandatory) or informative (non-mandatory) to define their application.