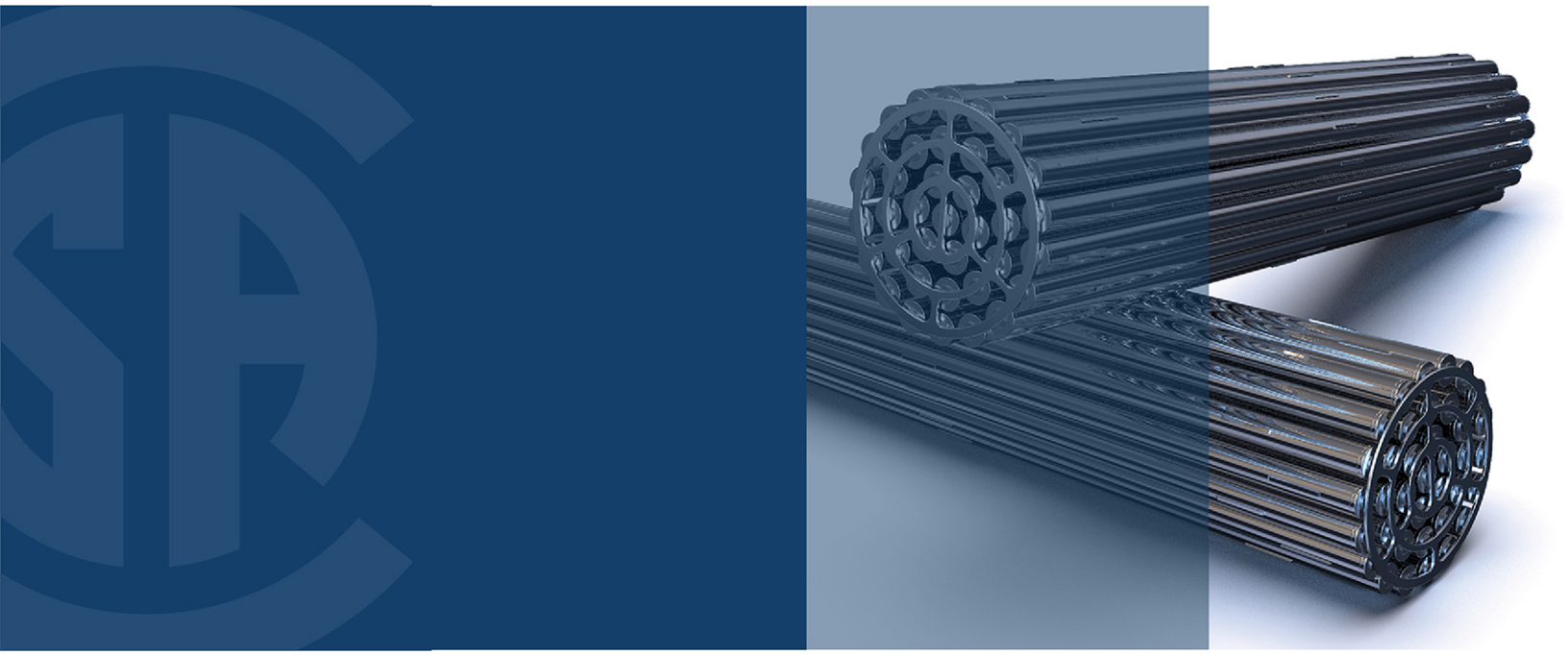
CSA GROUP™

CSA N290.7:21

Cyber security for nuclear facilities



Legal Notice for Standards

Canadian Standards Association (operating as "CSA Group") develops standards 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 Group 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 Group does not warrant the accuracy, completeness, or currency of any of the information published in this document. CSA Group makes no representations or warranties regarding this document's compliance with any applicable statute, rule, or regulation.

IN NO EVENT SHALL CSA GROUP, 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 GROUP HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, INJURY, LOSS, COSTS, OR EXPENSES.

In publishing and making this document available, CSA Group 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 Group accepts no responsibility whatsoever arising in any way from any and all use of or reliance on the information contained in this document.

CSA Group is a private not-for-profit company that publishes voluntary standards and related documents. CSA Group 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 Group and the users of this document (whether it be in printed or electronic form), CSA Group 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 Group's and/or others' intellectual property and may give rise to a right in CSA Group and/or others to seek legal redress for such use, modification, copying, or disclosure. To the extent permitted by licence or by law, CSA Group 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 Group 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 Group 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 Group 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 Group; 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.

Standards Update Service

CSA N290.7:21
October 2021

Title: *Cyber security for nuclear facilities*

To register for e-mail notification about any updates to this publication
- go to **www.csagroup.org/store/**
- click on **Product Updates**

The **List ID** that you will need to register for updates to this publication is **2428461**.

If you require assistance, please e-mail **techsupport@csagroup.org** or call 416-747-2233.

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

CSA N290.7:21
Cyber security for nuclear facilities

Published in October 2021 by CSA Group
A not-for-profit private sector organization
178 Rexdale Boulevard, Toronto, Ontario, Canada M9W 1R3

To purchase standards and related publications, visit our Online Store at ***www.csagroup.org/store/***
or call toll-free 1-800-463-6727 or 416-747-4044.

ISBN 978-1-4883-3159-6

Contents

Technical Committee on Reactor Control Systems, Safety Systems and Instrumentation for Nuclear Power Plants

C. M. Daniel	AECOM, Richmond Hill, Ontario, Canada *Category: Service Industry*	*Chair*
J. R. Burnett	Framatome, Pickering, Ontario, Canada *Category: Service Industry*	*Vice-Chair*
A. Au	Ontario Power Generation, Pickering, Ontario, Canada *Category: Owner/Operator/Producer*	
R. K. Black	TC Energy, Toronto, Ontario, Canada *Category: Service Industry*	
M. Buckler	Bruce Power, Tiverton, Ontario, Canada	*Non-voting*
Q. B. Chou	Canadian Power Utility Services Ltd (CPUS), Toronto, Ontario, Canada *Category: Service Industry*	
J. Coady	Bruce Power L.P., Tiverton, Ontario, Canada *Category: Owner/Operator/Producer*	
B. J. Coulas	Kincardine, Ontario, Canada *Category: General Interest*	
J. M. Cuttler	Cuttler & Associates Inc, Mississauga, Ontario, Canada	*Non-voting*
C. Darling	Framatome, Pickering, Ontario, Canada	*Non-voting*
M. Derewonko	Bruce Power L.P., Tiverton, Ontario, Canada	*Non-voting*

I. Dimitrov	Ontario Power Generation Inc, Pickering, Ontario, Canada	*Non-voting*
H. Gaber	University of Ontario Institute of Technology (UOIT), Oshawa, Ontario, Canada *Category: General Interest*	
D. L. Gillard	Richmond Hill, Ontario, Canada	*Non-voting*
R. Ion	MeV200 Consulting Inc, Mississauga, Ontario, Canada *Category: Supplier/Fabricator/Contractor*	
U. Kukreti	Markham, Ontario, Canada	*Non-voting*
W. K. Lam	Toronto, Ontario, Canada *Category: General Interest*	
A. Lee	Independent Electricity System Operator (IESO), Toronto, Ontario, Canada *Category: Government and/or Regulatory Authority*	
L. C. Luckhardt	Baker Hughes - Dresser, Dundas, Ontario, Canada *Category: Supplier/Fabricator/Contractor*	
J. Miller	Ontario Power Generation, Pickering, Ontario, Canada	
S. A. Miller	Port Elgin, Ontario, Canada	*Non-voting*
G. Mirzaei	SNC-Lavalin Nuclear Inc., Mississauga, Ontario, Canada *Category: Supplier/Fabricator/Contractor*	
C. D. Moore	NB Power Nuclear, Point Lepreau, New Brunswick, Canada *Category: Owner/Operator/Producer*	
B. Nangia	Nuclear Promise X (NPX), Mississauga, Ontario, Canada	*Non-voting*

H. Payne	BWXT Nuclear Energy Canada Inc, Peterborough, Ontario, Canada *Category: Supplier/Fabricator/Contractor*	
A. Persaud	Canadian Nuclear Safety Commission (CNSC), Ottawa, Ontario, Canada	*Non-voting*
H. Shah	Epoch Alliance, Markham, Ontario, Canada	*Non-voting*
J. Sigetich	Canadian Nuclear Safety Commission, Ottawa, Ontario, Canada *Category: Government and/or Regulatory Authority*	
G. Sutton	Canadian Nuclear Laboratories Limited (CNL), Chalk River, Ontario, Canada *Category: Owner/Operator/Producer*	
B. Willemsen	NB Power Nuclear Corporation, Fredericton, New Brunswick, Canada	*Non-voting*
E. Stencel	CSA Group, Toronto, Ontario, Canada	*Project Manager*

Subcommittee on Cyber Security for Nuclear Facilities

H. Shah	Epoch Alliance, Markham, Ontario, Canada	*Chair*
R. Altagracia Poueriet	Bruce Power, Tiverton, Ontario, Canada	
M. Benjamin	Toronto, Ontario, Canada	
R. L. Brown	Canadian Nuclear Laboratories, Fredericton, New Brunswick, Canada	
K. da Silva	Ontario Power Generation, Pickering, Ontario, Canada	
M. Daley	Canadian Nuclear Laboratories, Fredericton, New Brunswick, Canada	
B. Fichman	Ontario Power Generation Inc, Pickering, Ontario, Canada	
K. Fraser	SNC Lavalin (Candu Energy Inc), Mississauga, Ontario, Canada	
S. Hilts	Bruce Power, Tiverton, Ontario, Canada *Chair of the Subcommittee during development of this edition, 2018-2020*	
C. H. Jung	Canadian Nuclear Safety Commission (CNSC), Ottawa, Ontario, Canada	
B. Latimer	Bruce Power, Tiverton, Ontario, Canada	
E. Macasias	Ontario Power Generation, Pickering, Ontario, Canada	
H. Medina	Hatch Ltd, Mississauga, Ontario, Canada	

G. Mogorean	Kinectrics Inc, Toronto, Ontario, Canada	
H. Payne	BWXT Nuclear Energy Canada Inc, Peterborough, Ontario, Canada	
D. Rogalski	Ontario Power Generation, Pickering, Ontario, Canada	
M. Rowland	Sandia National Laboratories, USA	
J. A. Sladek	Canadian Nuclear Safety Commission, Ottawa, Ontario, Canada	
J. Thompson	Bruce Power, Tiverton, Ontario, Canada	
H. Thompson	NB Power Nuclear Corporation, Lepreau, New Brunswick, Canada	
B. Tomczyk	AECOM, Whitby, Ontario, Canada	
E. Stencel	CSA Group, Toronto, Ontario, Canada	*Project Manager*

In addition to the members of the Subcommittee, the following people made valuable contributions to the development of this Standard:
K. Chen
G. Khul
K. Lei
M. MacDonald
P. Mahdian
J. Plourde
G. Steeves
T. Vaughan
B. Weiss
F. Zeuchner

Preface

This is the second edition of CSA N290.7, *Cyber security for nuclear facilities.* It supersedes the previous edition published in 2014 under the title *Cyber security for nuclear power plants and small reactor facilities*. Changes to this edition include:

a) replacement of the term "vulnerability" with "susceptibility";
b) replacement of the previous Clause 7 (Cyber security architecture) with a new Clause 7 (Defensive cyber security architecture) which defines a Defensive Cyber Security Architecture concept based on groupings (called Zones) of cyber assets having the same or similar requirements for cyber security;
c) revision of Clause 8 (Security controls) to improve the criteria for CEA control applicability (eliminated Table 1) in response to industry experience with the previous edition;
d) enhanced the Supply Chain requirements in Clause 9 (Lifecycle management);
e) inclusion of a new Clause 10 (Cyber security incident response); and
f) removal of the former Annex A (Definitions for cyber security controls) and inclusion of applicable content in the body of the Standard as guidance.

The CSA N-Series Standards provide an interlinked set of requirements for the management of nuclear facilities and activities. CSA N286 provides overall direction to management to develop and implement sound management practices and controls, while the other CSA Group nuclear Standards provide technical requirements and guidance that support the management system. This Standard works in harmony with CSA N286 and does not duplicate the generic requirements of CSA N286; however, it may provide more specific direction for those requirements.

This Standard reflects the operating experience of the Canadian nuclear power industry.

Users of this Standard are reminded that the design, manufacture, construction, commissioning, operation, and decommissioning of nuclear facilities in Canada are subject to the provisions of the *Nuclear Safety and Control Act* and its supporting Regulations.

This Standard has been prepared by the Subcommittee on Cyber Security for Nuclear Facilities, under the jurisdiction of the Technical Committee on Reactor Control Systems, Safety Systems, and Instrumentation of Nuclear Power Plants, and the Standards Steering Committee on Nuclear Standards.

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 Standard 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 Standard.*
4) *To submit a request for interpretation of this Standard, please send the following information to inquiries@csagroup.org and include "Request for interpretation" in the subject line:*
   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) *where possible, phrase the request in such a way that a specific "yes" or "no" answer will address the issue.*

   Committee interpretations are processed in accordance with the CSA Directives and guidelines governing standardization *and are available on the* Current Standards Activities *page at standardsactivities.csa.ca.*

5) *This Standard is subject to review within five years from the date of publication. Suggestions for its improvement will be referred to the appropriate committee. To submit a proposal for change, please send the following information to inquiries@csagroup.org and include "Proposal for change" in the subject line:*
   a) *Standard designation (number);*
   b) *relevant clause, table, and/or figure number;*
   c) *wording of the proposed change; and*
   d) *rationale for the change.*

CSA N290.7:21
Cyber security for nuclear facilities

1 Scope

1.1

This Standard covers the cyber security of new and existing nuclear power plants (NPPs) and small reactor facilities.

Note: *This Standard may provide guidance for nuclear facilities other than NPPs and small reactor facilities, using a risk-informed graded approach.*

1.2

This Standard addresses cyber security for systems and components which perform or impact:

a) functions important to nuclear safety;
b) nuclear security functions;
c) emergency preparedness functions;
d) safeguard functions; and
e) those auxiliary functions which, if compromised, exploited, or failed, could adversely impact Item a), b), c), or d).

Note: *This Standard may be applied to other functions, such as those related to production reliability.*

1.3

This Standard pertains to the securing of cyber essential assets to protect against cyber attacks resulting in consequential degradation or loss of ability to perform their intended function, the compromise of their availability, integrity, and the loss of confidentiality of information that they store, process, or transmit.

1.4

This Standard does not apply to business systems (e.g., work management) and offline engineering systems, except for business systems that are part of the secure development environment at the time of development.

1.5

In this Standard, “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; and “may” is used to express an option or that which is permissible within the limits of the standard.

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 (nonmandatory) to define their application.

