21st Annual Conference of the Canadian Nuclear Society
Toronto, Ontario, Canada / June 11-14, 2000

N286.7-99, A Canadian Standard Specifying Software Quality Management System Requirements for Analytical, Scientific, and Design Computer Programs and its Implementation at AECL

By
R. Abel
R&M Abel Consultants Inc.

Acknowledgement

The author wishes to recognize the contributions of the many individuals, too numerous to mention here, who gave of their time and expertise to develop N286.7-99 over nearly 15 years of effort.

The author acknowledges with thanks the assistance of AECL staff in the Corporate QA Department under the direction of B. Shalaby (Chief Engineer) and S.S. Dua (Director, Corporate QA) at its Sheridan Park site in preparing this paper. Records Center staff provided valuable help by making available historical records concerning the development of the N286.7-99 standard.

Introduction

Analytical, scientific, and design computer programs (referred to in this paper as "scientific computer programs") are developed for use in a large number of ways by the user-engineer to support and prove engineering calculations and assumptions. These computer programs are subject to frequent modifications inherent in their application and are often used for critical calculations and analyses relative to safety and functionality of equipment and systems.

A large number of guides and standards are available from many publishing organizations in Canada and internationally, providing guidance and specifying quality management system requirements for software in general. CAN/CSA-ISO 9000-3-98 [1], the CSA Q396 series of Canadian standards [2], and a series of documents published by IEEE [3] are examples.

However, very little specific information is available addressing the development, modification, and application of computer programs that are used to perform design calculations and analyses of nuclear power plant systems. There are unique validation issues associated with scientific computer programs. Very little guidance is available how

to manage existing computer programs, so-called legacy codes, developed using informal and sometimes undocumented quality management practices.

N286.7-99 [4] was developed to establish appropriate quality management system requirements to deal with the development, modification, and application of scientific computer programs. N286.7-99 provides particular guidance regarding the treatment of legacy codes.

Brief History of N286.7-99

Some of the Challenges

The subcommittee developing the N286.7-99 standard (the CSA N286.7 subcommittee) had to address a number of issues. Since the start of the Canadian nuclear power plant program in the early 1960s key stakeholder organizations have developed a large number of computer programs to perform scientific and engineering calculations. These organizations used differing practices to develop, maintain, and use such computer programs. They followed the best practices of the day, often without defining formal quality management systems in this area.

These so-called legacy codes represent a substantial investment by the Canadian nuclear industry. Key stakeholder organizations gained confidence in these computer programs through continuing use and improvement, comparison against research and development data, and the performance of actual CANDU nuclear power plants.

As a result, the CSA N286.7 subcommittee had to strike a balance between:
(a) requiring that legacy codes be discarded totally and replaced with newly developed computer programs;
(b) imposing no quality management system requirements on the basis that legacy codes had been developed prior to the promulgation of any applicable standards in Canada; and
(c) specifying a reasonable and practical set of requirements to achieve the necessary confidence that results produced by such legacy codes were reliable, and that continued use, modification, and configuration management of legacy codes be brought under adequate control.

The CSA N286.7 subcommittee also had to achieve a consensus on the quality management system requirements applicable from now on to the development, modification and use of scientific computer programs. Again a reasonable balance had to be struck between giving programmers and users “free reign” to apply individually unique practices and imposing excessive constraints that eventually would prove costly and ineffective.

Chronology of Some Key Events

The development of N286.7-99 spans a period of nearly 15 years from May 1984 until the publication of N286.7-99 as a regular standard in March 1999. Some of the key events during this period are described briefly.

In May 1984 the CSA N286 Technical Committee on Overall Quality Assurance for Nuclear Power Plants establishes a working group to look into the need for a new quality assurance standard for scientific computer programs. The working group reports to the CSA N286 Technical Committee in April 1986. It recommends that a new standard be developed and submits a tentative outline for such a standard.

In June 1987 the CSA N286 Technical Committee establishes a subcommittee to develop a standard within the CSA N286 series, to be designated N286.7. Stakeholder organizations are invited to name representatives to the CSA N286.7 subcommittee.

By October 1992 a draft of N286.7 is established. The CSA N286 Technical Committee holds a recorded vote in June 1993 resulting in two negative ballots with the understanding that work will continue to improve the standard. At a subsequent meeting in February, 1994 the CSA N286 Technical Committee decides to issue N286.7 as a Preliminary Standard as a means of resolving the two negative ballots. A letter ballot formally approves the issue of N286.7 as a Preliminary Standard in March 1994. (A Preliminary Standard is a document issued for trial use for a period of two years.)

In the course of the CSA N286.7 subcommittee's continued efforts to improve the standard a meeting takes place in June, 1996 where the Atomic Energy Control Board (AECB) raises a number of concerns particularly regarding the treatment of legacy codes. In April 1997 the AECB restates its concerns formally in a letter together with some proposed resolutions. The CSA N286.7 subcommittee meets to consider the AECB's concerns but fails to find acceptable resolutions.

At the direction of the CSA N286 Technical Committee a meeting is held between AECB representatives and executive members of the CSA N286 Technical Committee. Specific actions are agreed to addressing the AECB's concerns. In February 1998 the CSA N286.7 subcommittee issues proposed revisions to the standard in response to the actions agreed to in November 1997 inviting final comments from stakeholder organizations.

In May 1998 the CSA N286.7 subcommittee issues the draft standard to the Canadian Standards Association for approval by letter ballot. The results of the ballot are available in September 1998. One negative ballot by the AECB requires resolution. A special meeting of the CSA N286 Technical Committee is held in November 1998 where this

negative ballot is resolved. The first edition of N286.7-99 as a regular standard is published in March 1999.

Relationship of N286.7-99 to Other Standards in the CSA N286 Series of Standards

The suite of standards in the CSA N286 series [5] is illustrated in Figure 1. This series of standards defines the quality management system requirements across all major phases of the nuclear power plant life cycle. N286.7-99 is part of this series and applies during any nuclear power plant life cycle phase where scientific computer programs are used.

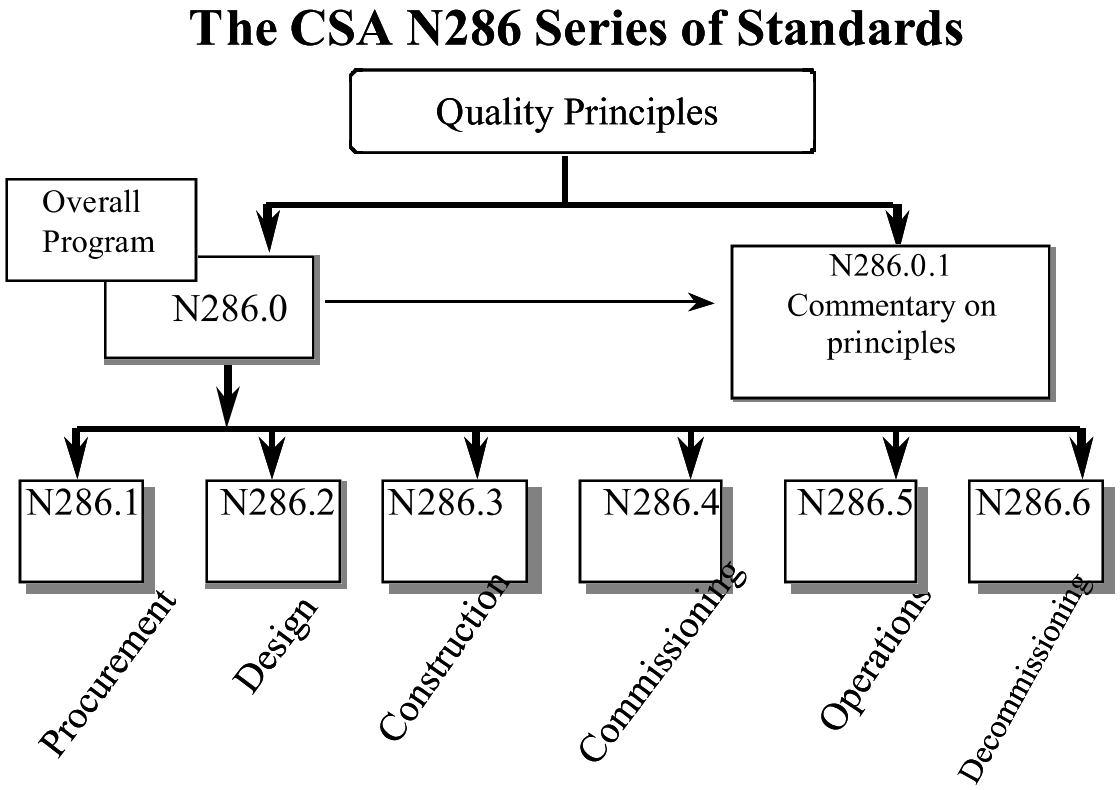

Figure 1

N286.7-99 complements, and has to be used in conjunction with, the requirements in the other standards in the CSA N286 series. For example, N286.7-99 relies on these other standards to specify requirements for general quality management system elements such as:

(a) the definition and implementation of an organization's overall quality management system (quality assurance program);

(b) the definition of the organizational structure;

(c) work planning and control;
(d) independent assessments (quality assurance audits);
(e) records management; and
(f) formal quality program reviews.

Key Features of N286.7-99

Scope of N286.7-99

N286.7-99 specifies the requirements for quality management systems applicable to the design, development, maintenance, modification, and use of computer programs used in nuclear power plant applications to perform or support:
(a) design and analysis of safety related equipment, systems, structures, and components;
(b) deterministic and probabilistic safety analyses and reliability studies;
(c) reactor physics and fuel management calculations; and
(d) transfer of data between computer programs or pre- and post-processing calculations associated with (a), (b), and (c) above.

N286.7-99 does not apply to computer programs such as:
(a) real-time computer programs used to control nuclear power plant safety systems and operational control systems;
(b) commercially available database management and spreadsheet programs. However, programmed applications using such tools are within the scope of N286.7-99.
(c) commercially available graphics and computer assisted drafting (CAD) computer programs. However, programmed applications using such tools are within the scope of N286.7-99.
(d) commercially available compilers, interpreters, and computer operating systems; and
(e) commercially available mathematical library subroutines.

Finally, the interpretation or application of results produced by scientific computer programs in design and analysis activities are outside the scope of N286.7-99. The quality management system requirements applicable to such activities are normally given in CAN/CSA N286.2-96 [5].

Organizational Responsibilities

All organizations developing, modifying, or using scientific computer programs have to incorporate the requirements of N286.7-99 into their existing quality management systems, which are based on one or more of the CSA N286 series of standards as required by the scope of their work. Responsibilities specifically applicable to scientific computer programs include:

(a) employing only qualified persons to perform work involving the development, modification, and use of scientific computer programs.

(b) ensuring that computer programs have a known "quality pedigree" satisfying the requirements of N286.7-99, when they are procured from software vendors not required to comply with any CSA N286 standard. The principal objective of this requirement is to ensure that only reputable software developers are considered who maintain defined quality management systems of a rigor comparable to that demanded by N286.7-99.

(c) appointing a "Primary Holder" who holds overall responsibility in the organization for maintaining a specific computer program. The appointment of a "Primary Holder" establishes a single point of responsibility for controlling computer program maintenance activities, maintaining configuration management, and for managing the communication with users.

Applicability

N286.7-99 provides specific direction regarding the use of legacy codes. (Note that this approach is similar to the treatment of legacy codes recommended in Section 9 of NUREG/BR-0167 [6]).

The requirements on computer program design and development and its associated documentation do not apply to computer programs developed prior to the issue of N286.7-99, i.e., legacy codes, provided no changes have been made to such computer programs. Such computer programs can continue to be used for performing substantial[1] new safety and licensing analyses if the user organization:
(a) identifies to which extent the legacy code conforms to N286.7-99 requirements on computer program design and development and its associated documentation;
(b) provides adequate justification why a legacy code can be used in spite of noncompliance with some requirements on computer program design and development and its associated documentation;
(c) indicates what verification activities will be performed and the verification needed; and
(d) provides a timetable for performing the specified verification activities.

Classification of Changes

N286.7-99 provides for two levels of requirements applicable to the treatment of computer program changes, depending on whether a change is classified as significant or not. Such a classification has to be justified and documented.

---

[1] Examples of substantial safety or licensing analyses are:
[1] (a) Analysis of shutdown system effectiveness; and
[2] (b) Analysis used to show that allowable radiation release limits are not exceeded.

A great deal of discussion took place during the development of N286.7-99 how best to define when a change should be considered significant. No universally applicable set of criteria could be defined that would distinguish significant changes to computer programs from those that are not significant. Therefore, the standard allows for a degree of judgment to be applied. Some guidance in arriving at a suitable classification is provided by way of a set of specific examples of changes that could potentially be considered significant. The set of examples provided is not considered all-inclusive. They include:

(a) changes to the theoretical background of underlying mathematical models;
(b) changes in the solution techniques used, such as the finite element method or numerical integration method;
(c) the addition of new functional capabilities;
(d) changes in data structure; or
(e) change in the programming language used.

Change Control

A prerequisite to making changes to any part of a computer program is to have access to all information necessary to understand the purpose and design of the computer program version being changed. Also, a system must be in place to control changes. Such a change control systems must have the following characteristics:

(a) the reasons for changes have to be identified;
(b) the computer program version being modified has to be identified and a new version identification has to be established;
(c) proposed changes have to be reviewed and approved;
(d) significant changes have to be implemented according to a dedicated development plan;
(e) a requirements specification has to be prepared for significant changes;
(f) changes and their verification have to be documented. This includes an assessment of the impact of significant changes on other parts of the computer program; and
(g) the new version has to be archived and formally released for use.

Computer Program Design and Development

The N286.7-99 requirements related to computer program design and development apply to any development activities, i.e., the design and development of both new computer programs and significant computer program changes. These requirements are not structured to cater to any particular software development model, such as the waterfall, spiral, or prototyping model. The underlying premise is that the principal stages of software design and development are generally common to all software development models.

N286.7-99 expects any computer program design and development process to include the following stages:

(a) Problem Definition

The physical problem has to be described that the computer program is expected to solve.

(b) Development Plan

The computer program design and development is expected to follow a prescribed plan, which is kept current as the work proceeds.

(c) Theoretical Background

The theoretical and mathematical basis for the solution of the problem has to be established.

(d) Requirements Specification

The requirements specification is used to define essential characteristics of the computer program.

(e) Computer Program Design

The design of the computer program has to be developed in such a way that it demonstrably addresses all the specified computer program requirements.

(f) Computer Program Coding

Coding includes translating the computer program design into a chosen computer language, debugging the resulting computer program, and integrating the modules into a complete program. Good programming practices are recommended in a non-mandatory appendix.

(g) Analysis Uncertainties

Uncertainties about the outputs of a computer program may arise due to causes such as the nature of mathematical models and numerical solution techniques, the accuracy of empirical correlations, or inaccuracies of library functions. The causes of such uncertainties have to be identified. Where possible, the magnitude of such uncertainties has to be estimated or such uncertainties have to be related to overall uncertainty allowances established during the validation process.

N286.7-99 requires that qualified and independent reviewers (those who did not actively participate in performing the work under review) verify the correctness of the information provided on the theoretical and mathematical basis, the design requirements, the scientific computer program design, and the computer program coding.

Configuration Management

N286.7-99 requires that the integrity and traceability of a particular set of computer program components be maintained. This typically includes the source code, operating system, compiler, library functions, object modules, executable code and any instructions

used with the compiler or linker, and applicable computer program documents. The standard treats any change to one or more computer program components as a new configuration that has to be given a new and unique identity according to a defined naming convention.

Validation

The term "validation" has various meanings in published standards and guides on computer program design and development. For example, "validation" is often used to describe the activities performed at the end of the development cycle to confirm that the completed and integrated computer program complies with the requirements established at the beginning of the development cycle. The practices established in the Canadian nuclear industry ascribe a different meaning to the term "validation". Therefore, N286.7-99 provides a definition of the term that is consistent with accepted practice in the Canadian nuclear industry.

As used in this standard, "validation" refers to the act of comparing the results of a given computer program with measurements during the nuclear power plant commissioning phase, experimental data, or known analytical or numerical solutions, so that the accuracy or uncertainty of a particular application of a given computer program can be determined. The standard also requires that conclusions regarding validation take into account the accuracy of the information against which the computer program is being judged.

Use of Computer Programs

Experience has taught that care has to be applied in the proper use of complex computer programs used for design and analysis work in order to obtain credible results. N286.7-99 specifies a number of minimum requirements in this area to ensure that:

(a) computer programs are validated for the intended use;

(b) analysis results do not fall outside the documented range of the computer program's applicability;

(c) input data are verified for consistency with the physical system or process analyzed;

(d) derivations and sources of input data are documented to facilitate independent review;

(e) configurations of the computer program and input data are identified so that the results can be reproduced;

(f) results produced by a computer program are reviewed to confirm that they are reasonable;

(g) user qualifications are specified and any required training is provided to minimize any undesirable effects on the computer program results due to particular user habits.

N286.7-99 also formalizes a number of requirements to ensure ongoing communication between the "Primary Holder" and the user community. The "Primary Holder" is required to advise users about:
(a) new developments in the computer program; and
(b) errors or deficiencies in the computer program or related documents.

At the same time users and computer program developers are required to keep the "Primary Holder" informed of any errors or deficiencies that they identify in the computer program or related documents.

N286.7-99 addresses the question of computer program transfers from one location to another. It requires that the receiving group confirm receiving the specified version of the computer program. The receiving group also has to confirm that the computer program executes as expected at the new location.

Documentation

N286.7-99 divides computer program related documents into two groups. One group supports the computer program design and development phases. The second group assists users of a computer program in its application.

The standard refers to individual documents in specifying the requirements for both sets of documents. However, the standard permits combining one or more documents into one so long as the content, review, and approval requirements for the combined documents are satisfied.

Design and Development Documents

N286.7-99 requires that design and development documentation include:
(a) A problem definition – a description of the problem to be solved;
(b) A development plan – plan(s) indicating the design and development work breakdown structure, the sequence and timing of activities, development tools and techniques to be used, review, testing, verification, and validation activities and methods, how independence is achieved between performers and verifiers, how nonconformances are resolved, work to be performed by subcontractors, and the methods used to control the interfaces between contributors to the computer program;
(c) A theory manual – a description of the theoretical and mathematical foundations of the computer program; this includes identifying the mathematical equations, assumptions and constraints, solution techniques, and empirical correlations; (this document is also considered part of the set of application related documents.)
(d) A requirements specification – specifies the name and functions of the computer program and the requirements applicable to hardware, computer program and user interfaces, operating systems, computational speed, portability, file size and type, input

and output, data structure and data flow, programming language, physical or mathematical models, numerical algorithms, error detection and handling, accuracy targets, programming practices;
(e) A design description – describes the computer program design and how specified requirements are met;
(f) Verification reports – records of the verification activities and their results;
(g) A programmer's manual – describes program flow and structure, how theory is translated into coding, how to modify and maintain the computer program, and programming conventions;
(h) A validation report - records the activities and results to show the accuracy or level of uncertainty in using a computer program for a particular application. Such a report is required at the end of the design and development life cycle and also whenever the computer program is applied to analyze a problem. Therefore, validation reports also form part of the set of application documents.

Application Documents
N286.7-99 specifies the following minimum set of application documents:
(a) A computer program abstract – provides a summary of the purpose, capabilities, operating environment, and limitations of a computer program;
(b) A theory manual – describes the theoretical and mathematical foundations of the computer program;
(c) A user's manual – provides information necessary to properly execute a computer program;
(d) A validation report – See item (h) under "Design and Development Documents";
(e) Version tracking record – documents the relationship between different versions of a computer program recording its evolution over time.

Consistent with the requirements in other standards of the CSA N286 series, N286.7-99 requires that all documents be subject to review and approval. Qualified individuals perform the reviews, who did not prepare the documents.

Implementation of N286.7-99 at AECL

AECL recognized the importance of implementing an effective quality management system to control both the development and use of scientific computer programs. It wanted to have in place such a quality management system based on a recognized standard as soon as it became available. Therefore, AECL chose to initiate an implementation process in the fall of 1996 in anticipation of the approved version of N286.7-99 by using a nearly final draft of the standard, dated August 13th, 1996. The implementation process was completed in the spring of 1999.

AECL's implementation process was designed to address the following objectives:

(a) Develop a practical quality management system that addresses the requirements of N286.7-99;
(b) Communicate the requirements of N286.7-99 to those involved with the design, development, modification, and use of scientific computer programs;
(c) Identify and take advantage of existing quality management system elements and supporting infrastructures;
(d) Identify current issues of working with scientific computer programs, and concerns about the requirements of N286.7-99;
(e) Identify gaps in existing quality management systems against N286.7-99 requirements; and
(f) Promote acceptance of the new quality management system by involving those in its creation who would have to perform their work under this system.

The first step in the implementation process consisted of a series of seminars held at all AECL sites attended by staff working with scientific computer programs. A senior line manager introduced each session, stressing the importance of this quality improvement initiative and confirming AECL senior management's support.

Various speakers then reviewed:
(a) basic quality management systems principles and concepts;
(b) the consequences of poor software quality management systems as illustrated by a number of computer program failures published in the open literature; and
(c) the requirements of N286.7-99 (August 13th, 1996 draft).

Each seminar concluded with an extensive discussion with the audience. Questions and concerns about the N286.7-99 requirements and about working with scientific computer programs were addressed. Information was gathered about existing quality management system elements and supporting infrastructures. Gaps in existing quality management systems against N286.7-99 requirements were identified and documented.

The second step in the implementation process involved establishing a quality management system development team. The team was charged with preparing a corporate level quality assurance manual giving an overview of AECL's scientific software quality management system. The team was also responsible for preparing a set of company wide procedures defining the processes used to manage the development, maintenance, and use of scientific computer programs.

This team was lead jointly by a senior line manager responsible for implementing the requirements of N286.7-99 and by a senior member of AECL's Corporate QA Department who provided expertise in the CSA N286 series of Canadian quality assurance standards and who was familiar with AECL's quality management systems and

their documentation. Team members were line staff representing all major areas in AECL where scientific computer programs are developed, maintained, or used. This included staff from safety and analysis, design, and project functions.

The team used existing processes to prepare the corporate scientific software quality assurance manual and its supporting procedures. Individual team members were given responsibility for preparing sections of the manual and for drafting procedures in their specific area of expertise.

The layout of the quality assurance manual followed closely the clauses in N286.7-99 to demonstrate compliance with the standard. Consistent with AECL requirements the manual includes a cross-reference table that correlates the clauses of N286.7-99 with the corresponding sections in the corporate scientific software quality assurance manual and with relevant supporting procedures. This table provides readers with an easy guide to detailed procedures governing applicable work processes.

Company wide procedures were developed to define the steps in key work processes. Team members made as much use as possible of any existing procedural documents by upgrading them to be acceptable as company wide procedures. The layout and format of the procedures complies with the requirements of existing AECL procedures. In particular, the work processes are described in "play script[2]" format, in flowcharts, or using a combination of these two methods.

Extensive use was made of a formal review and comment process to confirm the adequacy of the corporate scientific software quality assurance manual and its supporting procedures. Draft copies of the documents were distributed to knowledgeable managers and staff across AECL. The reviewers were required to submit written comments to the team members responsible for particular draft documents. Authors prepared and documented proposed resolutions to the reviewers' comments. Authors were required to achieve consensus with reviewers on acceptable resolutions of their comments.

The third step in the implementation process consisted of the formal rollout of the corporate scientific software quality management system. A series of training sessions were held to introduce AECL staff to the scientific software quality assurance manual and its supporting procedures. All documents describing AECL's scientific software quality management system were made available on the AECL Intranet. Where needed, hard copies of these documents were also distributed to selected areas.

[2] "Play script" format is used to describe sequentially both the activities and who performs them, requiring a minimum of text. This style of describing a sequence of actions is adapted from the way the dialogue and actions are described in a theater play that the actors are expected to perform.

The final step in the initial implementation of the corporate scientific software quality management system was taken by individual line organizations. They developed and executed their own implementation plans for bringing existing practices in line with the company wide quality management system.

As part of its quality management system AECL has established a Code Management Panel and a Computer Program Change Control Board.

The Code Management Panel reports to the AECL Executive Committee and performs an oversight role. It provides advice and guidance regarding:

[1] the development and application of AECL scientific computer programs; and

[2] the formal endorsement of scientific computer programs that meet the requirements of N286.7-99.

The Computer Program Change Control Board operates under the auspices of the Code Management Panel. It evaluates proposed changes to scientific computer programs used by AECL.

AECL has now taken steps to align its corporate scientific software quality assurance manual and its supporting procedures with the approved version of N286.7-99 published in March 1999.

Summary

N286.7-99 provides guidance to the Canadian nuclear industry on the definition and implementation of quality management system elements applicable to scientific computer programs. The standard provides what is considered both adequate and practical direction regarding the treatment of legacy codes. The Canadian nuclear regulatory agency has actively participated in the development and approval of N286.7-99 as a Canadian standard. Therefore, it also satisfies Canadian nuclear regulatory requirements applicable to quality management systems for such computer programs.

AECL has defined its quality management system elements addressing the requirements of N286.7-99. It has achieved this implementation taking into consideration the users' concerns from across the company. AECL has also taken advantage of current information technology, including its Intranet, to make available quality management system documents across the company. The strategy used in the definition, development, documentation, and communication of this set of quality management system elements at AECL has served as a model for the introduction of company wide quality management systems addressing the requirements of other CSA N286 sub-tier standards.

References

[1] CAN/CSA-ISO 9000-3-98, Quality Management and Quality Assurance Standards – Part 3: Guidelines for the Application of ISO 9001:1994 to the Development, Supply, Installation, and Maintenance of Computer Programs, Canadian Standards Association/CSA International

[2] CAN/CSA-Q396.0-91, Guide for Selecting and Implementing the CAN/CSA-Q396-89 Software Quality Assurance Program Standards

CAN/CSA-Q396.1.1-89, Quality Assurance Program for the Development of Software Used in Critical Applications

CAN/CSA-Q396.1.2-89, Quality Assurance Program for Previously Developed Software Used in Critical Applications

CAN/CSA-Q396.2.1-89, Quality Assurance Program for the Development of Software Used in Noncritical Applications

CAN/CSA-Q396.2.2-89, Quality Assurance Program for Previously Developed Software Used in Noncritical Applications

Canadian Standards Association/CSA International

[3] IEEE Standards Collection; Software Engineering, 1993 Edition, The Institute of Electrical and Electronics Engineers, Inc.

[4] N286.7-99 – Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants, Canadian Standards Association/CSA International

[5] CAN/CSA N286.0-92, overall Quality Assurance Requirements for Nuclear Power Plants

N286.0.1-92, Commentary on the Principles for Quality Assurance Programs of CSA N286 Series Standards

CAN/CSA N286.1-96, Procurement Quality Assurance for Nuclear Power Plants

CAN/CSA N286.2-96, Design Quality Assurance for Nuclear Power Plants

N286.3-99, Construction Quality Assurance for Nuclear Power Plants

CAN/CSA N286.4-M86, Commissioning Quality Assurance for Nuclear Power Plants

N286.5-95, Operations Quality Assurance for Nuclear Power Plants

N286.6-98, Decommissioning Quality Assurance Program Requirements

N286.7-99 – Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants

Canadian Standards Association/CSA International

[6] NUREG/BR-0167 – Software Quality Assurance Program and Guidelines, February, 1993, U.S. Nuclear Regulatory Commission