Software Quality Assurance (SQA) of ACR Computer Codes

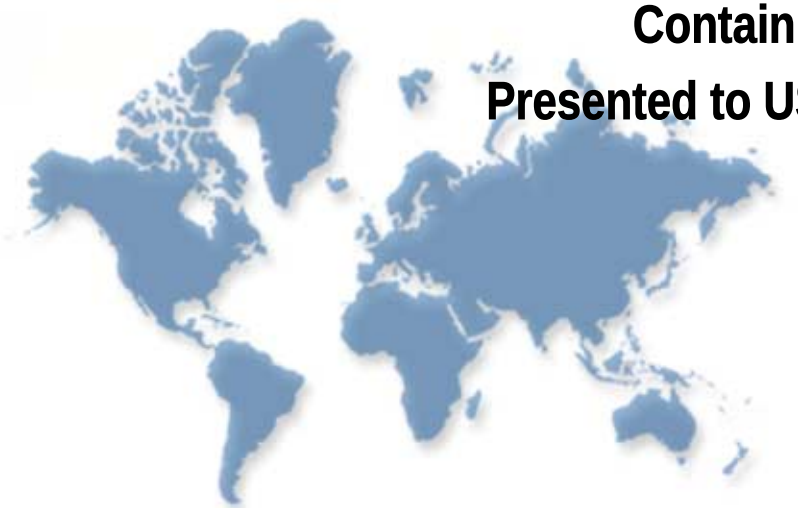
D.J. Richards, Manager

Containment & Thermalhydraulic Analysis

Presented to US Nuclear Regulatory Commission

Washington DC

May 15-16, 2003



AECL TECHNOLOGIES INC.

Outline

- Objectives
- Background
- Elements of AECL's SQA Program
  - Responsibilities
  - Requirements for Computer Programs
  - Computer Program Design and Development
  - Acquisition of Analytical, Scientific and Design Computer Programs
  - Configuration Management
  - Change Control
  - Validation
  - Use of Computer Programs
  - Documentation
- Summary

Background

- The Canadian Standards Association (CSA) published "Quality Assurance of Analytical, Scientific, and Design Computer Programs for Nuclear Power Plants", N286.7-99 in March 1999
- AECL published 00-01913-QAM-003, "Quality Assurance Manual for Analytical Scientific and Design Computer Programs in September 1999, and revised the document in 2001 March to address comments internal to AECL as well as external (Canadian Nuclear Safety Commission (CNSC))

Background (concluded)

- 00-01913-QAM-003 is supported by a number of AECL procedures:
  - Document Review and Comment
  - Computer Program Design and Development
  - Use of Analytical, Scientific and Design Computer Programs
  - Acquisition of Analytical, Scientific and Design Computer Programs
  - Change Control
  - Verification
  - Validation
  - Configuration Management
  - Documentation
  - ….. and others

Elements of AECL's SQA Program

- Responsibilities
- Requirements for Computer Programs
- Computer Program Design and Development
- Acquisition of Analytical, Scientific and Design Computer Programs
- Configuration Management
- Change Control
- Validation
- Use of Computer Programs
- Documentation
- Verification Processes

Responsibilities

- **AECL is responsible to ensure SQA activities are performed in accordance with the N286.7-99 Standard**
  - **This is accomplished through adherence to the AECL Manual and specific AECL Procedures**
  - **Verification of compliance is established through audits (Internal as well as third-party External Audits (e.g, CNSC, Clients))**
  - **Activities are monitored by the office of AECL's Chief Quality Officer (Dr. A.M.M. Aly) who reports directly to the President and CEO of AECL (Mr. Robert Van Adel)**

Computer Program Design and Development Steps

1) Problem Definition
2) Development Plan
3) Theoretical Background
4) Requirements Specifications
5) Design
6) Coding
   - A verification step is required for 3) to 6)

Problem Definition

- **Problem to be solved is documented**
  - **Rationale and objectives are given**
  - **If a change is being made to an existing program, the reason why the change is necessary will be clearly stated**

Development Plan

- **The Development Plan:**
  - Gives a breakdown the computer program development into manageable tasks and the assignment of related responsibilities, including review and approval authority
  - Provides the sequence and timing of activities to be performed, key milestones, and outputs
  - Identifies the development tools, techniques, and methodologies to be used
  - Provides the review, testing, verification, and validation activities to be performed, the methods to be used, and the rationale for their selection
  - Gives the means to achieve independence between those performing and verifying activities

Development Plan (concluded)

- **The Development Plan:**
  - **Provides the means to resolve nonconformances**
  - **Identifies the computer program components to be developed by subcontractors and the applicable quality assurance programs**
  - **Provides the methods to control interfaces between contributors to the computer program development, including customers**
  - **Identifies the documents to be produced as part of the development process, a description of their purpose and content, and the identification of responsibility for producing, reviewing, and approving documents**
  - **Identifies the configuration management methods**

Theoretical Background

- **The Theoretical Background provides:**
  - **The theory and mathematical equations**
  - **The assumptions and constraints**
  - **The solution techniques and the rationale for selecting these techniques, such as accuracy requirements and other limitations**
  - **Any empirical correlations, their range of application, and associated uncertainties**
  - **Applicable existing references**

Requirements Specification

- **The Requirements Specification gives:**
  - **the name of the computer program**
  - **the functions of the computer program**
  - **hardware, computer program, and user interface requirements**
  - **operating system requirements**
  - **computational speed requirements**
  - **portability requirements**
  - **file size and type requirements**

Requirements Specification (concluded)

- The Requirements Specification gives:
  - Input and output requirements
  - Data structure and data flow requirements
  - Programming language
  - Imposed physical or mathematical models or numerical algorithms
  - Error detection and handling requirements
  - Accuracy targets
  - Requirements on programming practices

Design Description

- **The Design Description gives:**
  - **An identification of the algorithms**
  - **Computer program structure, including data structures and program flow**
  - **Description of modules and module interfaces**
  - **Library functions (if applicable)**

Coding

- Recommended Programming Practices are available
- Verification methods are defined in the Development Plan
- Examples:
  - Walkthrough
  - Independent review of computer program coding
  - Mathematical analysis of computer program functions
  - Unit testing

“Legacy” Computer Programs

- Are those developed prior to 1999 (prior to promulgation of the Standard, N286.7-99)
  - Qualification Plan must be generated
  - Qualification Report is generated that verifies the Qualification Plan has been completed
  - All further development must conform to the Software Development Cycle:
    - Problem Definition
    - Development Plan
    - Theoretical Background
    - Requirements Specifications
    - Design
    - Coding

Qualification Plan

- Qualification Plan is a document which specifies actions/plans/schedule to qualify a legacy code used for substantial new safety or licensing analysis
- Activities covered by this plan include:
  - identify the extent to which the computer program conforms with the design and development requirements from the AECL Software Quality Assurance Manual
  - provide justification for non-conformances with the same design and development requirements
  - define what verification activities will be performed and the verification needed
  - identify the time scale over which verification activities will be performed

Acquisition of Analytical, Scientific and Design Computer Programs

- **Process:**
  - Generate Problem Definition and a request to purchase to the procurement function
  - Receiving Inspection ensures software and documentation are as specified in Purchase Order, then sends package to Primary Holder of Code
  - Primary Holder performs series of acceptance tests (delivered by supplier)
    - Results are archived
    - Verification Report is generated
  - Software is placed under Configuration management
  - Program is then validated for the given application

Configuration Management

- Configuration components include:
  - source code
  - operating system, compiler, library functions, object modules, executable code, and instructions used with the compiler and linker
  - computer program documents
- Each configuration is uniquely identified
- Any change to one or more components constitutes a new configuration

Change Control

- A Change Control System requires that:
  - The reasons for changes be identified
  - The version to be modified be specified and a new version identification proposed
  - Changes be classified as significant or not, and justification provided
  - Proposed changes be reviewed and approved
  - A change control plan (i.e., Development Plan for changes) be produced for significant changes
  - A Requirements Specification be produced for significant changes

Change Control (concluded)

- **A Change Control System shall require that:**
  - **Changes and their verification be documented, including an assessment of the impact of significant changes on other parts of the computer program**
    - **This is normally done through using an "Acceptance Test Suite", to test the new version**
  - **The new version be archived and released for use**

AECL Code Management Panel

- **Company-wide policy and direction setting committee for Scientific, Design and Analysis computer programs**
  - **Members – senior managers from all parts of AECL involved with development or use of the codes**
  - **Meets 6-8 times per year**
  - **Oversees operation of**
    - **Code Center**
    - **Computer Program Change Control Board (CPCCB)**

AECL Code Center

- Responsible for all (non-commercial) transfers of AECL software to external organizations
  - Universities
  - Research organizations
- Executable copies of the Codes are licensed, not sold

AECL Computer Program Change Control Board (CPCCB)

- **Responsibilities**
  - Reviewing and endorsing proposals to make any significant modifications to any Scientific, Design or Analysis code
  - Assessing impact of changes on other codes or parts of AECL
  - Supports line management in prioritizing the use of AECL resources (funds and staff)
  - Meets as needed to respond to submissions

Use of Computer Programs

- **AECL ensures the proper use of Computer Programs by ensuring that:**
  - **Computer programs are validated for the intended use**
  - **Only those physical states are analyzed that are within the documented range of the computer program's applicability**
  - **The input data is verified to ensure that it adequately represents the physical system or process analyzed**
  - **The derivations and sources of input data are documented in a form that facilitates independent review**

Use of Computer Programs (concluded)

- **AECL ensures the proper use of Computer Programs:**
  - **The configuration of the computer program and the input data are identified so that results can be reproduced**
  - **The results produced by the computer program are reviewed to confirm that they are reasonable**
  - **User qualifications are specified and the necessary training is provided to minimize the effect of user dependency**

QA Procedures for Code Calculations -1

Input data:

- Formal procedures in place to ensure the completeness, accuracy and validity of the calculations or analyses.
- The accuracy of the results are verified by one or more of the following:
  - Alternate methods
  - Testing
  - Experience
  - Well described additional measures
- Each calculation is accompanied by a Technical Calculations Report that documents that the verifier is qualified for the task, the verification methods and the verification findings

QA Procedures for Code Calculations - 2

- **Analysis Basis Documents**
  - In addition to the checking of input data, assumptions and methodology are also verified
  - An Analysis Basis (AB) document contains all analysis methods, assumptions and data, with justification for their use and application for a particular analysis
  - The Analysis Basis document is formally peer-reviewed
  - The comments from reviewers, and their accepted dispositions, are kept on file as part of the formal documentation

Documentation

- **Two types of documentation:**
  - **Design and Development**
  - **Application (i.e. User)**

Documentation: Design and Development Documents

- **Problem Definition**
- **Development Plan**
- **Theory Manual *(also Application Document)***
- **Requirements Specification**
- **Design Description**
- **Verification Report**
- **Programmer's Manual**
- **Validation report *(also Application Document)***

Documentation: Application Documents

- Computer Program Abstract
- Theory Manual
- User's Manual
- Validation Manual
- Version Tracking Record

Computer Program Abstract

- **The Computer Program Abstract includes:**
  - **The computer program name**
  - **The version identification**
  - **A brief description of the problem solved**
  - **The applicable configuration components**

Theory Manual

- **The Theory Manual includes:**
  - **The theory and mathematical equations**
  - **Assumptions and constraints**
  - **Solution techniques and the rationale for selecting these techniques, such as accuracy requirements and other limitations**
  - **Any empirical correlations, their range of application, and associated uncertainties**
  - **Applicable existing references**

User's Manual

- The User's Manual includes:
  - Instructions on installing and running the computer program
  - A description of features, capabilities, and options including options available to users and recommendations on nodalization schemes
  - A description of input and output
  - A description of error and warning messages, their interpretation, and recommended corrective action
  - Identification of embedded and default values
  - A description of limitations and restrictions
  - Sample cases that illustrate the use of components and modules

Validation Manual

- **A Validation Report includes:**
  - **A statement of the application for which the computer program is being validated**
  - **A description of the methods used**
  - **Identification of data against which validation was performed**
  - **Computer program input and output**
  - **Validation Results**
  - **An assessment of validation results with respect to computer program accuracy and uncertainty allowances**

Version Tracking Record

- **A Version Tracking Record includes:**
  - **Identification of the version that was modified and of the new version**
  - **Reasons for the change**
  - **Significance of the change and the basis for the categorization**
  - **The Identity of those who made the change**
  - **The release date of the new version**
  - **The modified computer program components**

Version Tracking Record (concluded)

- **A Version Tracking Record includes:**
  - **A description of changes, and reference to documents containing more detailed information where appropriate**
  - **The methods used to verify and, as appropriate, validate the new version**
  - **The location where the computer program is archived**
  - **A list of other computer program documentation that has been revised**

Summary

- AECL processes for SQA have been described
- AECL processes are based on CSA N286.7-99, and are defined by an AECL Manual and associated Procedures
- Compliance with these procedures for Analytical, Scientific, and Design Computer programs is mandatory in AECL
- Compliance is verified through extensive Internal Audits as well as External Audits


AECL
TECHNOLOGIES INC.