Verification, Validation, and Control of Automated Calculational Applications Subject to ASME NQA-1 Quality Assurance Requirements

Katie Phillips, Jaime Rickert, Charles A. Waggoner
Institute for Clean Energy Technology, Mississippi State University
205 Research Blvd, Starkville, MS 39759

ABSTRACT

Mississippi State University (MSU) Institute for Clean Energy Technology (ICET) tests filters for use in nuclear facilities, and therefore must have a quality assurance program that meets the Quality Assurance Requirements for Nuclear Facility Applications (NQA-1) as specified by project sponsors. One of the final stages of testing these filters is to reduce the data collected during testing. MSU-ICET has implemented a procedure for Automated Calculational Applications (ACA) to ensure that the NQA-1 requirements concerning data reduction are met. Initially, the software developer creates the data reduction ACA software based upon specifications provided by the project sponsor. The data reduction verifier then produces an ACA Package that contains the unique name and version, the general purpose and requirements of the ACA, the procedure for using the ACA, the Verification and Validation (V&V) Report, an ongoing list of any changes, and any equations or references used in the creation of the ACA software. Once the ACA has been verified and validated, it is transferred to the data reduction computer and a Transfer of ACA analysis is performed and documented to ensure the same results are produced on the data reduction computer. An ACA Checklist of all of the items required in the ACA Package is completed by an independent reviewer. Upon completion of the ACA Package for each data reduction ACA, all necessary requirements of NQA-1 are documented, reviewed, and approved.

INTRODUCTION

Currently, the work being performed by Mississippi State University (MSU) Institute for Clean Energy Technology (ICET) includes testing full scale filters, both axial flow and radial flow, in addition to the testing of flat sheet media coupons. Project sponsors must qualify MSU-ICET's quality assurance program to ensure the program meets the Requirements for Nuclear Facility Applications (NQA-1) since the filters being tested are either presently in use or are being qualified for use in nuclear complexes. The NQA-1 standard is an American Society of Mechanical Engineers (ASME) safety-driven standard, rather than an International Organization for Standardization (ISO) process-driven standard. It applies to activities "that could affect the quality of nuclear material applications, structures, systems, and components of nuclear facilities." [1]

Certain NQA-1 requirements are not applicable to the work being performed at MSU-ICET since MSU-ICET is not the manufacturer of the filter units being tested. However,

other requirements of the NQA-1 standard must be focused on in depth. One of the several quality-affecting items of the MSU-ICET program is the process for reducing data that is collected during testing. This data reduction process is subject to software quality assurance requirements of NQA-1 and are addressed through a quality assurance procedure for Automated Calculational Applications (ACA).

REQUIREMENTS

The requirements from Part I of NQA-1 that pertain to the data reduction process used at MSU-ICET include Requirement 3, Design Control, and Requirement 11, Test Control. Part II, Subpart 2.7, Quality Assurance Requirements for Computer Software for Nuclear Facility Applications, supplements the requirements of Part I and is used in conjunction with those requirements for the “development, operation, maintenance, and retirement of software.” [1]

Software Design

NQA-1 Requirement 3, Design Control, imposes that the software requirements are identified and documented. Sufficient documentation of design and development includes the objective of the software. Other requirements, as specified by Requirement 3, include background information as applicable, indication of assumptions, details of the computer identification, and review and approval. Additionally, Subpart 2.7 establishes that documentation such as software design requirements, instructions for computer program use, test plans, and results shall be controlled, planned, and performed in an orderly manner. Additionally, each software program shall be uniquely identified and given a proper revision number to allow for more precise identification for each configuration. [1]

Verification and Validation

NQA-1 Requirement 11, Test Control, requires that the test procedures for computer programs used for operation provide demonstration of performance over the functional range, as well as an evaluation of the technical adequacy of the program. This evaluation can be demonstrated through hand calculations, calculations using comparable proven programs, or empirical data and information from technical literature. Within this evaluation, the computer program shall be verified to show that the results from any mathematical models produced are correct. Furthermore, it shall be shown that the mathematical models used are valid models for the problem at hand. Specifically, Subpart 2.7 requires that the acceptance testing demonstrate, as appropriate, that the computer program properly handles abnormal conditions and events as well as credible failures, does not perform adverse unintended functions, and does not degrade the system either by itself, or in combination with other functions or configuration items. [1]

NQA-1 Requirement 3, Design Control, necessitates that a competent individual other than the one who originally designed the program perform the verification. “The extent of verification and the methods chosen are a function of the complexity of the software, the degree of standardization, the similarity with previously proved software, and the importance to safety.” According to Requirement 11, the verifier may choose to use alternate calculations, reviews of design, performance tests, or any combination thereof to verify the software. Among the items that shall be listed in verification test results are the computer program tested, date of tests, tester or data recorder, simulation models used (where applicable), results and applicability, action taken in connection with any deviations noted, and person evaluating the test results. [1]

Configuration Control

Once the software is established for operational use, it shall be controlled with approved application documentation, access control specifications, problem reporting and corrective action, in-use tests, and the configuration change control process. NQA-1 Requirement 11, Test Control, establishes that in-use test procedures be developed and performed after the software is installed on a different computer or when significant changes have been made to the operating system. It shall also be noted that manual in-use tests be made periodically to check for program errors that could affect the data produced. [1]

NQA-1 Requirement 3, Design Control, states that formal documentation of changes made to software shall include a description of the change, the rationale for the change, and the identification of affected software. Subpart 2.7 specifies that the configuration change control shall include initiation, evaluation, and disposition of a change request, control and approval of changes prior to implementation, and requirements for retesting and acceptance of the test results. Additionally, a method shall be established to handle a problem that is determined to be an error, specifically how the error relates to various elements of the software, how the error impacts past and present use of the program, how the corrective action impacts activities, and how to avoid the error once the corrective action is implemented. Other changes may include requests to make the software more user-friendly or revisions to design based on the development of the software requirements. Each change to software shall by authorized by the appropriate personnel and verified before put in use. These changes shall be documented such that they can be traced back to the appropriate version of the software design. [1]

Upon retirement of a program or design, the software shall be removed and the use of the software shall be prevented. [1]

AUTOMATED CALCULATIONAL APPLICATIONS

Automated Calculational Applications (ACA) are defined to encompass commercially available software packages used to automate repetitive hand calculations or provide

graphical representations of test data. MSU-ICET currently uses Microsoft Excel for all quality-related data reduction as allowed by para. 302 of Subpart 2.7. [1] The ACA is designed and created by the Software Developer based on the specifications of any current contracts. Once the ACA is created, the Data Reduction Verifier compiles an ACA Package to document the validity of results produced by the ACA. The ACA Package for each ACA includes a detailed listing of each sheet within the workbook, sufficient instruction for utilizing the ACA, a Verification and Validation (V&V) Report, a life cycle document of all updates and modifications, and references for equations and restrictions. In the case that an ACA is comprised of multiple workbooks, each of those workbooks has a separate listing, procedure, and V&V Report within a joint ACA Package.

ACA Software Design

The ACA Design and Development process is the operation of transferring the concept of data reduction and the data reduction requirements as specified by project sponsors into an ACA. This is performed at the computer by the software developer, and results in the development of the data reduction ACA for operation and use.

The ACA Package for each data reduction workbook begins by stating the full file name, including the file extension. The “Purpose” section provides a brief overview of the workbook at hand, including requirements set forth by project sponsors. The following “Description” section of the ACA Package breaks down each sheet within the workbook. The design of each sheet includes whether or not the user needs to manually input any information, whether the sheet is visible or hidden, any plots or data tables, and a general understanding of what calculations are performed on that sheet. Background information, indication of assumptions, and details of the computer identification are documented in the V&V Report section of the ACA Package.

As required by NQA-1 Subpart 2.7, each ACA Package contains rigorous instruction for utilizing the ACA. This section begins by stating the accessible sheets and where the user can find any outside information (e.g. a laboratory notebook) that needs to be manually typed or copied into the data reduction ACA. The step-by-step instructions that follow detail how to copy raw data into the ACA, exact cells that require manual entry, and any formatting that may need to be changed (e.g. updating headings of plots, resizing plot axes).

Verification and Validation Report

The V&V Report is also included in the ACA Package. The V&V Report explains how the data reduction ACA software has been verified and/or validated. For the purposes of testing at MSU-ICET, validation shall specify that the correct formulas are being used, and verification shall check the results of the ACA and ensure that the requirements have been met.

Currently, MSU-ICET pre-verifies each ACA before applying it for operational use. The data reduction verifier performs a series of hand calculations to document sufficient test cases to accept that the ACA is acting as it has been designed. The data reduction verifier chooses to check the first, last, and some appropriate middle cells in a column of like-formulated cells since the software developer uses the auto-fill option to create spreadsheets. Cells that have unique formulas are tested individually. The acceptability (e.g. results agree within 0.01%) of the results and the actual percent difference of any discrepancies between the ACA output and the results of hand calculations performed by the data reduction verifier are recorded in the V&V Report upon completion of testing of the ACA.

It is understood that calculations, such as averaging, are used within the ACA, and they do not need to be further explained in the V&V Report. However, equations and formulas used beyond the scope of averaging schemes and call functions need to be sufficiently documented. The V&V Report directs the reader to an attachment that outlines each of those equations. If any constraints or restrictions are present, they are documented at this time.

All equations used in the ACA that are not call functions or averaging schemes are documented accordingly. Included in the ACA Package is the “Origin of Equations.” Here, each formula is stated, and its variables are defined. The description of each equation contains any references and restrictions and specifies exactly where the equation is used within the ACA.

The data reduction verifier also ensures that the ACA is performing to the previously established standards and criteria of acceptability upon installation of the ACA onto the data reduction computer. This is documented through an attachment to the Automated Calculational Applications procedure titled “Transfer of ACA,” which is further discussed in a later section.

Configuration Control

A number of steps are taken to prevent the misrepresentation of data. As a measure to prevent a user from editing cells that contain formulas, sheets that do not contain any end results or plots are locked, password protected, and hidden from view. Additionally, those sheets that do not require any input but may have plots or tables that the user needs access to are locked and password protected but kept visible. On the sheets that require manual inputs, all cells except those requiring input are locked and password protected. The password is chosen and known only by the Quality Assurance Coordinator (QAC).

All official data reduction used to produce quality data is performed on the specified data reduction computer. This computer is password protected and kept in a locked room. The software custodian is the only person with access to the “Admin” account on the computer. The computer is setup such that anyone on the “User” account cannot overwrite or save a different version of the ACA. Additionally, a copy of the ACA is

saved on a separate flash drive and maintained in a 2 hour fire-rated filing cabinet. Furthermore, the data reduction computer is disconnected from the internet to prevent any updates to software that may put the ACA at risk of being changed without approval.

To ensure that the ACA performs in the same manner on the data reduction computer as the computer that it was originally tested and verified on, the data reduction verifier completes a Transfer of ACA report. This report includes the name and version of the ACA, a set of data to verify that the transfer is effective, and the acceptance criteria to deem the transfer successful. The data reduction verifier chooses a set of data that is representative of the ACA as a whole. Typically, this includes the end results of the calculations at hand. A Transfer of ACA report is also required when there are significant changes to the operating system on the data reduction computer. Upon approval by the data reduction verifier, the Transfer of ACA Report is attached to the ACA Package.

Before an ACA can be used to produce reportable data, an Independent Reviewer ensures that the ACA and corresponding ACA Package follow all guidelines and requirements by completing an ACA Checklist. The following set of points are used to approve the ACA for use:

- ACA Package contains sufficient listing of the organization of calculations between spreadsheets.
- ACA Package contains sufficient instruction for using the ACA.
- ACA Package specifies any operational environment specifics.
- ACA Package specifies which versions of workbooks were used to develop the ACA Package and test calculations of the ACA.
- ACA Package has an appropriate name and date or revision for the ACA.
- ACA Package contains applicable codes, standards, regulations, requirements, or instructions that establish acceptance criteria.
- ACA Package specifies any allowable or prescribed ranges for inputs and outputs in the ACA.
- ACA Package specifies which cells and sheets shall be protected and locked down by the QAC.
- Cells and sheets within the ACA are protected and locked down as required by the ACA Package.
- ACA has been tested and verified to perform to the acceptance criteria specified by the ACA Package, and a Validation and Verification Report has been generated and documented in the ACA Package.
- ACA has been installed on the data reduction computer by the Software Custodian, and a Transfer of ACA Report has been used to verify ACA is still performing to the previously established acceptance criteria.

The ACA Checklist is approved by the QAC and attached to the ACA Package.

In the case that any errors are found while using the ACA, the user notifies the software custodian, the data reduction verifier, and the QAC immediately. The software custodian shall remove the ACA from service until the impact on activities is determined and the problem can be resolved. When such errors are found or other modifications are in order, a Spreadsheet Change Request form is submitted. The person who issues the request includes the name and revision of the ACA, a description of the change requested, and the rationale for the change. Then the software developer evaluates the request and decides whether or not to make the change. If the decision is made to carry out the changes, the change request is assigned a unique number for traceability purposes. A new set of requirements and acceptance criteria are documented so that the data reduction verifier can reevaluate the ACA. Once the modifications have been documented (e.g. V&V Report, Transfer of ACA, ACA Checklist) and approved by the data reduction verifier and QAC, the ACA is once again ready for use.

A table is included in the ACA Package in order to track the versions of the ACA used to produce results. The table includes the name of the workbook to be edited, including the version number, the problem or reason for a change, the revised version number and date implemented, and the solution to any problem that was encountered. Each time any portion of the ACA is modified, it is documented here, and that portion of the ACA is re-verified and validated.

The software custodian ensures that the most up-to-date version of the ACA is in service on the data reduction computer. All previous versions of the ACA are retired by being removed from the data reduction computer. The software custodian is responsible for updating the software inventory list to reflect all changes.

CONCLUSION

MSU-ICET has put great effort into ensuring that all applicable requirements of NQA-1 have been met with regard to the use of software for data reduction. The procedure for proper development, verification, and control of the data reduction software has been documented in ICET's quality assurance procedure. The ACA Package is a detailed report listing all specifications of the necessary requirements of NQA-1 as specified by project sponsor.

ACKNOWLEDGEMENT

This work has been conducted with funding provided by Department of Energy (DOE) and Bechtel National, Inc. (BNI).

REFERENCES

1. American Society of Mechanical Engineers, 2008, “Quality Assurance Requirements for Nuclear Facility Applications (ASME NQA-1-2008) [Standard].”