Software Quality Assurance

Alternatives to the Safety Software Central Registry Toolbox

WP-2022-SAF-QA-SQA-001

Prepared By: Patrick Valentine Auer Digitally signed by Patrick Valentine Auer Date: 2022.04.27 14:14:59 -07'00'

Patrick V. Auer, Lawrence Livermore National Laboratory

Approved By: Teri Vincent Digitally signed by Teri Vincent Date: 2022.04.28 13:20:33 -04'00'

Teri Vincent, Consolidated Nuclear Services

SUMMARY:

The Department of Energy (DOE) Safety Software Central Registry (SSCR) Toolbox currently provides documentation for eight codes to support DOE contractors in performing calculations and in developing "*data used to establish the safety basis for DOE nuclear facilities and their operation, and to support the variety of safety analyses and safety evaluations developed for these facilities*". The original intent of the SSCR Toolbox, which was established in 2003, was to provide pedigreed versions of design and analysis codes used in safety analysis decisions that meet DOE Safety Software Quality Assurance requirements as defined in DOE Order 414.1D, *Quality Assurance,* including code-specific gap analysis documentation, guidance documents, and contact information. For the purposes of this white paper, the terms "code," "codes," "software," "application," and "applications" are considered equivalent.

The SSCR Toolbox currently lists eight codes, see Attachment 1, that have been vetted as meeting DOE software quality assurance requirements of DOE O 414.1D and the safety software guidance in DOE G 414.1-4, *Safety Software Guide*, Appendix B. However, qualification assessments of updates to new and improved versions of the Toolbox's existing codes have taken up to a decade to be conducted (e.g., the last qualification assessment of MELCOR was done 18 years ago). This often means that major revisions to the codes have been in common use for many years, while the code listed on the SSCR Toolbox is a much earlier version or has been classified as an obsolete version. Since DOE Complex sites are encouraged to use the Toolbox codes, which are considered to be a "safe haven" once they are acquired, and the code is brought into the site's QA/SQA program. The sites are reduced to using outdated codes unless the site is willing and able to conduct the qualification process. The use of the SSCR Toolbox codes does not negate the requirement to include them in the site's software quality assurance (SQA) program.

In April 2021, EFCOG began discussions around how to replace or update the "Toolbox" so that it would be more useful for the user community. These discussions centered around planning for the Safety Software Quality Assurance – Central Registry list of "Toolbox" codes to be discontinued and no longer supported by DOE Office of Environment, Health, Safety & Security. In addition, the Defense Nuclear Facilities Safety Board (DNFSB) requested additional information from DOE Office of Quality Assurance and Nuclear Safety Management Programs, EHSS-32 on how the SSCR is meeting the original intent of the Toolbox, as it was becoming clear that the codes are not the most current version and additional codes were not being added to the Toolbox. As a result of the DNFSB request, EHSS-32 is developing a project plan to address the necessary changes to the "Toolbox" method of maintaining qualification of safety analysis codes. EHSS-32 requested help from EFCOG to provide input to the project plan.

Contributions by:
Patrick Auer, LLNL
Chris Beaman, EHSS-32
Donna Riggs – Riggs Quality Consulting
David Louie – SNL
Gregory Baker – DOE NNSA NA-51
Dave Thoman – Amentum

PURPOSE:

The purpose or goal for this white paper is to provide alternatives to the SSCR Toolbox qualification process to aid EHSS-32 in the completion of a project plan to address how the SSCR Toolbox will be used and maintained in the future.

SCOPE:

The scope of this white paper is to provide recommended alternatives to the current SSCR Toolbox qualification method and maintenance of the codes.

DEFINITIONS:

None.

NARRATIVE:

The task team developed three alternative options for the SSCR Toolbox, which include the specified alternative, advantages, and disadvantages of each alternative. The alternatives are based on commonly accepted methods from organizations that are implementing the NQA-1 standard for qualification of software and qualification of suppliers of developed software.

In addition, to supplement the three alternatives, the task team recommends establishment of a DOE Complex user group forum to help implement the chosen alternatives as follows:

- Maintain consistent usage of the toolbox codes across the sites
- Ensure that the toolbox codes addition or deletion is adequately managed
- Recommend additional codes to be included
- Allow sites to show their usages and validation studies for that particular toolbox code
- Exchange lessons learned for issues relating to the use of the toolbox codes
- Enable a toolbox code qualification committee using EFCOG or DOE Organization Excellence process. Include SQA, DOE, oversight boards, SMEs, as applicable
- Drive consistency across the DOE complex for implementation of “otherwise acquired” and commercial grade dedication processes for software
- Provide opportunities for obtaining experience in qualifying codes

Options

<u>Information</u>
DOE Guide 414.1-4 defines Acquired Software as “generally supplied through basic procurements, two-party agreements, or other contractual arrangements. Acquired software includes commercial off-the-shelf (COTS) software, such as operating systems, database management systems, compilers, software development tools, and commercial calculational software and spreadsheet tools (e.g., Mathsoft MathCad and Microsoft Excel). Downloadable software that is available at no cost to the user (referred to as freeware) is also considered acquired software. Firmware is acquired software.”

ASME NQA-1 *Quality Assurance Requirements for Nuclear Facility Applications*, Subpart 2.7, uses the terminology of "Otherwise Acquired" for such software.

Option 1
Eliminate the SSCR Toolbox and treat all codes acquired from the SSCR and updates as "otherwise acquired" software and perform the necessary qualifications steps in accordance with Site's program.

Advantages
- DOE no longer needs to directly manage the qualification process if the SSCR goes away
- The software can be easily implemented and eliminates current uncertainty with SSCR expeditiously
- Sites could use and qualify which ever version(s) of the code they need. It would be up to the site to maintain usability for a specific version which is no longer supported by the developer, e.g., for design safety analysis calculations.
- DOE focuses on evaluating individual site's implementation of their approved SQA program through normal oversight processes

Disadvantages
- The SSCR goes away
- Increased costs to all sites using the code, including reluctance and pushback by different sites
- Increased documentation for each site
- Increased software testing and effort, which could be significant
- "Otherwise Acquired" and Commercial grade dedication processes for software at each site vary widely.
- Some sites do not have staff with adequate experience in qualifying code and performing commercial grade dedication (CGD) of software.
- The software being qualified is complex and may be difficult, at best, to qualify using these processes
- Redundant SQA plans for the same code across the sites of varying quality

Option 2
Have a site, or sites, manage the SSCR and perform the audits

Advantages
- Contract vehicle already in-place, just need funding and training
- Sites have the auditors and processes already in-place and could coordinate with the proposed DOE Complex user group forum to determine appropriate SMEs
- Does not require each site to individually qualify the codes for their specific uses, but at least one site-specific test would be expected at each site (e.g., installation verification)

Disadvantages
- Picking a site or sites
- SMEs are typically restricted to one site and SQA products reflect perspective of their site

- Will require some type of DOE oversight
- How much funding and where does the funding come from
- The funding may come project-directed activity or overhead, so the effort could vary year to year or project by project
- May use contractor staff that do not have Federal qualification for oversight of safety software
- May require Federal approval of the audit report or similar by an appropriately qualified Federal person

Option 3
DOE HQ, e.g., EHSS, could manage a direct support contract or similar vehicle to perform the audits of each code and maintain the SSCR.

Advantages
- The DOE contact would approve all audit reports
- DOE owns the process and SSCR, could support DNFSB or other inquiries
- If there is an existing contract with adequate scope of work, could be easier and faster
- Contractor could manage the SSCR inventory
- Draw SMEs or appropriate technical specialists from the sites to assist the direct support contractor
- Does not require each site to individually qualify the codes for their specific uses, but at least one site-specific test would be expected at each site (e.g., installation verification)

Disadvantages
- Need the contract vehicle, unless one is in place with appropriate scope
- Cost justification for a separate contract

If either option 2 or 3 is chosen, the SSCR would operate much like the Master Supplier List (MSL) (EFOCG's qualified supplier list). The list would only contain software that is developed specific to DOE facility needs by DOE Laboratories or other government organizations. The selected organization or contractor would perform an audit of the software developer's (e.g., DOE Laboratory or other government organization's) program once every 3 years; document an "annual evaluation" to ensure no significant changes to the QA or SQA program have been made in the years where no audit is performed; and maintain the list for users to access the current, or previously approved versions of the codes. The site would still need to "acquire" the code and incorporate it into the site's QA/SQA program.

Advantages
- Qualified (or Evaluated or Approved) Supplier lists are an established norm for NQA-1 based quality assurance programs
- Use NQA-1 qualified and certified lead audit personnel
- Does not require each site to individually qualify the codes for their specific uses but at least one site-specific test would be expected at each site (e.g., installation verification)
- The MSL approach is currently in use for maintaining a list of suppliers who have been audited to the QA standard as noted in the MSL for items or services which are to be procured from an NQA-1 or similarly approved source.

- Updates to the software do not require a supplier audit (though a significant change could trigger additional oversight)

Disadvantages

- May use contractor staff that do not have Federal qualification for oversight of safety software
- May require Federal approval of the audit report or similar by an appropriately qualified Federal person
- Funding has to be obtained and maintained
- The current EFCOG MSL process is somewhat difficult to implement, maintain, and obtain information from
- The SSCR cannot be “left alone” to run itself
- It could be difficult to obtain information needed to support site-specific use determinations

CONCLUSION:

DOE O 414.1D and NQA-1 allows for the qualification of software for use in a safety related application using various methods. The above listed alternatives could be used to support the DOE complex with adequate support, personnel, and funding.

REFERENCES:

None.

ATTACHMENTS:

Attachment 1 – List of Currently Qualified Toolbox Codes.

Attachment 1

List of Currently Qualified Toolbox Codes

CODE	VERSION	YEAR APPROVED	OWNER/DEVELOPER
ALOHA	V5.4.4	2014	National Oceanic and Atmospheric Administration (NOAA)
CFAST	V7.1.1	2017	National Institute of Standards and Technology (NIST)
EPIcode	V7.0	2004	Lawrence Livermore National Laboratory (LLNL)
GENII	V2.10.1	2013	Pacific Northwest National Laboratory (PNNL)
HotSpot	V2.07.01	2010	Lawrence Livermore National Laboratory (LLNL)
IMBA	IMBA Expert ™ USDOE Edition V4.0.28	2006	UK Health Protection Agency (HPA)
MACCS2	V1.13.1	2004	Sandia National Laboratories (SNL)
MELCOR	V1.8.5	2004	Sandia National Laboratories (SNL)