Software Quality Assurance

Better Application of DOE O 414 to “All” Software

WP-2021-SAF-QA-SQA-001

Prepared By: Patrick Valentine Auer

Digitally signed by Patrick Valentine Auer
Date: 2020.12.22 10:01:04 -08'00'

Patrick V. Auer, Lawrence Livermore National Laboratory

Prepared By: VERONICA CAMARILLO-MORRIS (Affiliate)

Digitally signed by VERONICA CAMARILLO-MORRIS (Affiliate)
Date: 2021.01.21 08:32:46 -07'00'

Veronica Camarillo-Morris, Los Alamos National Laboratory

Approved By: Vicki L. Pope

Digitally signed by Vicki L. Pope
Date: 2021.01.21 13:08:43 -08'00'

Vicki L. Pope, Lawrence Livermore National Laboratory

SUMMARY:

The goal of DOE O 414.1 is to make sure the software is good for intended use based on acceptance criteria. With that in mind, the *Better Application to "All" Software* sub-task group proposes modification to, along with justification, for changes to DOE O 414.1D when it is next revised.

The following actions would help clarify DOE O 414.1D requirements as they apply to software:

- Make it clear that the 10 work activities listed in Attachment 4 apply to all software.
- Include clarification in areas such as the definition of Software as an Item and commercial grade dedication as it applies to software.
- Use a consistent national consensus standard for all software to make it easier to coordinate across different entities (e.g., NNSA, NEA, NSE, multiple Labs, etc.) in developing software

Contributions by:
Greg Pope, LLNL
James Hylko, Paducah
Marylou Apodaca, SNL
Patrick Auer, LLNL
Stella McKirdy, INL
Veronica Camarillo-Morris, LANL

PURPOSE:

The purpose or goal for this white paper is to provide justification for a revision to DOE O 414.1D as it applies to software quality assurance (SQA). These changes would re-emphasize quality assurance (QA) and the 10 QA criteria to better clarify applicability to "all" software.

SCOPE:

The scope of the task was to provide recommended changes to DOE O 414.1D when the decision is made by DOE to revise the document, including clear points with justification.

Background:
The discussions for this whitepaper began at the Fall 2019 EFCOG QA Task Group meeting and are briefly summarized from various notes taken during that meeting as follows:

- SQA requirements apply to software beyond Safety Software. However, the requirement is only found in a note in 414.1D, Section 4.a.(2) and again in CRD, Attachment 1, Section 1.b. Therefore, the requirement to apply the 10 QA criteria to Non-Safety Software is often missed.
- DOE O 414.1D requires that all software meet the applicable QA requirements in Attachment 2 using a graded approach. However, no guidance is given as to what measure should be used for this graded approach or how best to apply it (*this issue will be addressed by a separate SQA sub-task project*).
- DOE O 414.1D applies to all work and the definition of work lists software development (including safety software) as either a defined task or activity. Therefore, "work" includes all software.
- Is there too much emphasis on safety software for nuclear and radiological facilities?
- The graded approach cannot be used to "grade quality assurance criterion to zero," which has the effect of eliminating all verifications of the requirements

- The definitions of software-related terms in DOE O 414.1D differ from the definitions in DOE O 200.1A (the Information Technology Management Order).
- The emphasis on NQA-1 is not balanced. For instance, there are categories of safety software that are not nuclear or radiological. These types of software, and all other Non-Safety software, can follow a standard other than NQA-1.

DEFINITIONS:

None.

NARRATIVE:

Why use or recommend NQA-1 or equivalent for Non-Safety Software?

The current requirements used for Safety Software follow NQA-1-2008 with the NQA-1a-2009 addenda, Part I and Subpart 2.7 or other national or international consensus standards that provide an equivalent level of quality assurance requirements as NQA-1-2008. Depending on the existing contract between each individual contractor and the DOE. Though not specified in 414.1D, NQA-1 Part I, Requirements 3 and 11 are most relevant to software. The justification for using NQA-1 as the core or default methodology for software is based on the principle that when we are dealing with any software at a DOE Facility that is ***in support of*** the operations, safety, maintenance and/or retirement of the facility it ***should be*** considered as part of the entire Software System Architecture (Infrastructure). Since all software within a facility works together as a cohesive Software System Architecture to ensure the success of operations, they should be treated accordingly.

Software Quality Assurance requirements have been re-iterated through several consensus standards and documents in order to drive home the importance of the activities needed to have quality software applications, and, in doing so, caused confusion on what the requirements actually mean. To simplify what is needed, it is best to focus on a single set of high-level requirements, which is what the EFCOG *Better Application to "All" Software* sub-task group believes DOE O 414.1 is trying to accomplish. In other words, having good software.

The approach would still apply the high-level software requirements listed in the DOE Order and NQA-1 based on risk and the graded approach as described in the contractor's DOE approved QA Program.

Existing Guidance:

DOE Guidance Document (DOE G 414.1-4) for DOE O 414.1 provides clear tables describing what is needed for both Safety and Non-Safety software in a graded approach as follows:

- Table 1. An Illustration of Quality Assurance (QA) Criteria (10 CFR 830 Subpart A and DOE 414.1C) Applicability to Software Quality Assurance (SQA) Work Activities
- Table 2. Grading Criteria and Facility Categorization Illustration
- Table 3. ASME NQA-1-2000 Cross Reference to DOE Software Quality Assurance.

Many people will argue that the rigor for Non-Safety Software using NQA-1 would be overkill, not necessary, and should only reference DOE O 414.1 quality assurance criteria. However, the application of a consensus standard such as NQA-1 to all software should be focused on the requirements for software use, acquisition, and development.

The focus for development of software should be on consideration of controls for Software

Requirements, Procurement of Software, Software Design, Software Quality Assurance Planning, Software Engineering, Configuration Management, Verification, Validation, Testing, Use, Problem Reporting, and Retirement.

The focus for acquisition of software should be on consideration of controls for the development of clear requirements (for Request for Proposal, specification, scope of work, etc.), pre-award supplier evaluation, acceptance of the software, maintenance, problem reporting or monitoring, installation testing, commercial grade dedication, and retirement.

CONCLUSION:

The following actions would help clarify the existing DOE O 414.1D requirements as they apply to software:

1. Make it clear that the 10 work activities listed in Attachment 4 apply to all software.

    - Remove the NOTE in DOE Order 414.1, Section 4.a.(2) and again in CRD, Attachment 1, Section 1.b, and make it clear this is required. Recommend this become Section 4.a.(2)(a) and again in CRD, Attachment 1, Section 1c, and state “All software shall meet applicable QA requirements in Attachment 2, using a graded approach.”

2. The order should include clarification in areas, such as, the definition of Software as an Item.

    - Clarify the definitions in the DOE Order applicable to software; coordinate these definitions with other, related DOE orders such as DOE O 200.1A.

3. Use a consistent national consensus standard for all software to make it easier to coordinate across different entities (e.g., NNSA, NEA, NSE, multiple Labs, etc.) when developing software.

    - Require the contractor to develop a matrix or similar document to be submitted along with their QAP to demonstrate that software is in compliance with the chosen standard.
    - Not enough detail in the DOE Order on implementing NQA-1 as a software standard, suggest a Table or other clarification on how to do that (e.g., focus on Requirement 3, 11 and Subpart 2.7).
    - Ensure that safety or security requirements are addressed as applicable when using various development methods, e.g., AGILE, or a modification of AGILE methods.
    - Ensure development methods remain flexible for all software.

REFERENCES:

NQA-1-2000 to 2008, and 2009a Requirements 3, 11, and Subpart 2.7

ATTACHMENTS:

None.