EFCOG SQA Spring 2021 MEETING NOTES

Wednesday April 21, 2021

Safety, Security, and Quality Moments, *Presenter Vicki Pope (LLNL):*

- Safety; spending lots of time on video conferences; take time away from the screen, stretch, take breaks.

Briefing on SQA-Related Standards and Orders Matrix, *Presenter Cristy Renner (Fluor BWXT):*

- Provide Pros/Cons Standards.
- Create a matrix of DOE Orders, Policies and Guidelines that have software-related guidance. The matrix shows an analysis of standards, orders, and policies related to software
- Look at how they complement, contradict, or add SW/SQA requirements to DOE O 414.
- List the "pros" and "cons" of each document and what to focus on.
- Better integrate DOE 414 with other DOE O and clarify if that should be an alternative.
- Many of the standards (e.g., CM standard) don't address software directly but the basics are there.
- Would like help analyzing additional standards/orders (see slides for list):
  - Looked at findings where this matrix would have helped.
    - Spreadsheets/Utility Calculations:
      - There are many utility calculation applications (based on spreadsheets) in use.
      - Most aren't recognized as software.
      - Some are not significant (e.g., tracking the office coffee funds); however, some are powerful, relied upon applications, even safety applications.
      - These need Configuration Management (CM), testing, and all the other SQA required practices of other safety or important software.
    - Many projects don't have requirements documents.
    - People need training/mentoring on SQA requirements and how to implement them.
    - Need guidance on legacy and freeware codes.
- The determination of the list was done by team members adding ones they felt were relevant to their sites or those referenced in the DOE Guide; if you know of orders/standards that have been missed, contact Cristy and let them know what they are.
- How can these documents help to understand software, test it, document it, based upon life cycle of software. Not enough people are trained in SQA. People don't understand how software is in everything. This can help us by creating a one-stop-shop to help compare this information. Keep matrix live.
- Reviewed SQA Audit/Assessment Findings or Observations:
  - Too many software owners/locations.
  - Utility calculations software per Guide (spreadsheets/databases):
    - Found over 1 million spreadsheets.
  - Software doesn't have documented Software Requirements Document.
  - Doesn't have documented Verification and Validation (V&V) Testing.
  - Didn't follow Software Development Life Cycle (SDLC).
  - 10 QA Elements were incomplete or non-existent.
  - SQA Audits/Assessments - assessors need to understand SQA requirements, testing, requirements, etc.
- For example, need to understand Configuration Management. Some do not relate to software exactly, even though, it does give us tasks to do for software.

- This matrix can help with SQA Audits and Assessments. Most everyone has, but there are duplicates of information. For example, utility calculations, people look at to help define as software. Guide is work tool, classification as software. For example, environmental simple calculations, how are you using them, are they used to build our environmental report to DOE, if so, it has to be tested. Spreadsheets can have human errors. Different factors as to why simple spreadsheets can be safety software. Spreadsheets are not being configuration management (CM) controlled. People didn't understand testing. Need training process.
- Some had no requirements. No documented V&V testing process. Need to come back and mentor people on testing. For example, environmental software from EPA still needs testing. People need to understand 10 elements of QA. Guide helps you to know what elements are needed.
- For Matrix, what documents are needed, break down, and guide people in how to use. Need to have more clarification on how documents are needed. Need more people to finish last documents.
- Start on White Paper in next few months. See some things lacking, provide issues and improvement opportunities.
- Can find Matrix at SQA Box folder, within T7 Software Orders and Standards.
- Should we keep old versions of documents such as DOE O 205.1B, 205.1C?
- Where are we Today
  - Have completed 16; have more to go; does anyone want to help?
  - Box site review; good collection

- Questions/Comments:
    - From Teri Vincent – some projects on old versions of documents. So, do need older versions of documents.
    - From Yvonne Deaton – Look at what versions of documents are referenced in your contract.
    - From Carol Olijar – Your task expanded to two tasks – Matrix, and info on each document in matrix, right?
      Answer: Yes, when combined two Task Groups into 1. We needed more robust, need relevance of Matrix.
    - From Yvonne Deaton – What was process to find orders? Can the mining tool be used to search for other documents; a lot of labs have tools that might be able to help. Suggest using mining tool, key areas missing such as testing. One lab has data mining tool.
      Answer: Did several ways, several sites, for example, references at end of guide, pull what was used to build guide. It would be great to use a mining tool.
    - From Vicki Pope – Do any of the labs have data mining tools? If so, please contact Christy or Teri Vincent.

Subtask Overviews

- Internet of Things – Orlando Ferrer, lead:
  - Focused on writing a guidance paper of devices that transmit data across the internet and what SQA practices should be applied.
  - New group focused on writing a set of procedures on IOT that can be connected to the internet that can be used on site.
- Toolbox Alternative – Pat Auer, lead:
  - What can replace or modify the current DOE Central Registry Toolbox
  - Will write a White Paper structured like a procedure for a process of qualifying tools for a Toolbox-like list
  - See slide for list of things they will be considering
  - It will take time for DOE HQ do decide if/how to dissolve or replace the current Central Registry
  - Need to address who will take responsibility for codes if there is a failure (e.g., liabilities)
  - Would need strong disclaimers as to what using a Toolbox code means and what activities the user site should perform prior to, during, and after use of these tools
- Testing Spreadsheets – Greg Pope, lead:
  - This group will prepare a White Paper with guidance on how/when to test spreadsheets
  - There are millions of spreadsheets being used today. Most are not tested
  - Even simple formulas need to be tested
  - Applications like Excel allows complex software to be built on top of the Excel base
  - Many of these are important, even safety applications.
  - Put a lot of important information on spreadsheets and don't really test them very well. Goal to document some guidance.
- Graded Approach – Lance Abbott and Jeni Turgeon, co-leaders:
  - This group will be finalizing the draft White Paper of graded approach to SQA.
  - Wanted to run by larger group before presented to DOE.

Sub-task Breakout Sessions, *See notes from Sub-group team leader:*

EFCOG "Toolbox Alternatives" Whitepaper subtask work group

Spring 2021 Meeting, Subtask breakout sessions #1 and #2, (April 21, 2021)

Participants (Blue highlights are sub task team members as of this time)
Pat Auer – Subtask lead, LLNL
Dave Thoman, subtask team member, Amentum
Chris Beaman, AU-32
Gregory Smith, LANL
Donna Riggs, Consultant
Diana Marquez, WRPS (will ask permission)
Gladys Udenta, NA-51
Gregory Baker, NA-51
David Louie, SNL
Kelli Presley-Thomas
Yevonne Deaton, DOE EM
==========

Discussion centered on a couple of key areas as follows:

Find out if there are alternatives to it. Narrow down focus and write white paper

Who is the audience for recommendations put forth from this whitepaper effort?

- DOE, AU-30 (Garret Smith)

What is the impact to your site if the toolbox goes away tomorrow?

- To be determined from below action items

1. Define problem statement – AU-30 does not have resources to move toolbox forward or maintain it "as is". Take the following actions
2. Develop Alternatives to the toolbox (Complete Draft by Fall 2021 EFCOG meeting)
3. Market / Communicate Alternatives

Action Items

1. Can AU share toolbox assessment report? If yes, Chris will share with group (C. Beaman)
2. Organize survey information PowerPoint add LANL information from Gregory Smith, including following questions as the last slide:
   - How many facilities/DSAs are using this software
   - How many users at each site/lab?
   - Current version, which version(s) do we need?
   - One or more than one SQA qualification at your site?
   - Why not use newer version? Cost prohibitive to redo DSA?
   - What happens if the toolbox goes away? Can you maintain your DSA? Impacts?
   - Are there sites that could be using the toolbox, but do not have access to it or use it

   Provide the presentation to Chris Beaman to discuss with AU-30, (D. Thoman, help as needed from P. Auer)

3. Maybe update survey based on input from AU-30 (D. Thoman)
4. Present results and input from AU-30 during tentatively scheduled May 26th subtask meeting, go over survey updates and information
5. Perform an impact analysis to determine any gaps this will leave the current Site software owners (i.e., what questions to ask)

==========

Highlights of discussions and talking points. This section will be used to capture thoughts and ideas going forward and to "work off" as the subtask evolves.

Disclaimer

- Each site must still follow their own SQA practices for use of the codes, e.g., testing, type of use, range of use, be familiar with the purpose and intended use of the code, etc.

Challenges

- No money to keep Central Registry going
- Users think if software is in the Central Registry, then they can use it with no testing
- Lack of expertise in the DOE field to even review new toolbox codes
- Gaps exist due to some software versions in ***current*** use are not consistent with the ***approved*** version causing additional verification/SQA time in the field

DOE AU support for toolbox

- Not likely to continue, no resources or bandwidth for maintaining the toolbox
- Not funded for staff to perform necessary tasks
- Could AU embrace the code as "recommended"
- Input for Users/Accident Analysis groups desired

Use of EFCOG MSL approach

- Discuss with supplier function to avoid pitfalls they encountered, e.g., funding, who is the lead, support from various organizations
- Trying to avoid a full-blown requalification of each code at each site, e.g., the code is treated as "pre-verified" similar to that purchased from an NQA-1 supplier
- Sponsor for the code or code champion

Toolbox Codes

- Legacy codes, how to update
- Used for DSA, cannot just retire the legacy codes
- Who maintains the actual code?
- Should there be a central code repository? Who would maintain this and where?
- Could this be added to EM IT Strategic Plan to fund as needed or recommended
- Add codes identified in CFRs?
- Exemptions for NIST owned and developed codes
- Identify sites who have used and tested a newer version of the code, can this be the baseline for the replacement of the Central Registry?
- Benefits of the toolbox, training in the code
- Who maintains the website? It depends… e.g., AU-30 hosts a web portal, website

Acquired Codes e.g., ANSYS, COMSOL

- Shared licensing costs?
- Sharing of information for qualification of acquired codes e.g., "otherwise acquired" and dedicated software

What is the scope of the toolbox codes?

- Current – "models or codes supporting DOE safety analysis"
- Should the scope be expanded to includes codes like Sierra, Melcor, Fuego?
- Other modern simulation codes

Other Issues

- Loss of expertise, retirement of personnel

Gaps exist due to some software versions in ***current*** use are not consistent with the ***approved*** version cause

Questions:

David Louie - timeline for getting different solution for CRTS? No timeline after DOE G is out but it will be after that most likely.
Carol - if we/users take over responsibility is the liability to contractor? Pat - need to look at that. Good idea to include letter from DOE.
Chris Beaman - part of it will include the approval of site safety basis.

Sub-task Breakout Sessions, *See notes from Sub-group team leader:*

Creating a Safety/Security Library for Your Code, *Presenter Greg Pope (LLNL):*

- Not easy to develop secure software for Agile. Can secure software be developed with Agile?
- A lot of the problem is due to missing requirements.
- Security is a requirement, but not always well defined. Make security requirements specific not implicit. Need to include security requirements into software requirements for Explicit and Implicit Requirements. May want something, but may not be able to describe item explicitly. Users may not be able to explicitly state all their explicit requirements.
- Avoid Phishing; get rid of hyperlinks in documents, embedded links. Browser Chrome can check links. Biggest vulnerability is people clicking on links within emails they receive – the email looks legitimate, but is not. Better to NOT imbed links in emails (very common hacker attack).
- If possible, open your own browser to access the company website (you time in the company name, don't copy / paste link address from the email). At LLNL, for email, there is link to report in Outlook, when hovering over link to email, to check to see if legitimate source. Fake email, report as phishing. If click on, bad move, need to take training. Fun way for employees to be careful about email.
- Install software that checks your system and identify all software running on your network. Compare this against things like the National Institute of Standards and Technologies (NIST) vulnerability database. Fix what is shown as vulnerable. S-bomb. Know vulnerabilities in software use. People don't know when they have sub-function software. Need to know what is running in your environment.
- Some mitigations to attacks must be performed at system/internet level.
- Greg wrote a white paper that has more details.
- Avoid "bolt-on" workarounds.
- Things discovered as security vulnerabilities, are found by manufacturer most often.
- Cyber attacks are big deal.
    - 94% malware delivered thru email.
    - Over 80% security breaches from phishing attacks.
    - Over 60% from unpatched vulnerabilities.
    - Attacks on Internet Of Things (IOT) have increased three fold since 2019.
- Agile is a Philosophy, not a process.
    - Everyone likes to say they are doing Agile, cool thing to do, even if they didn't understand Agile.
    - DOD came up with an Agile BS Detector – doing Agile or not. People say they are doing Agile, but not very well.
- Systemic Theoretic Process Analysis (STRA). Hazard analysis technique, alternative to FMEA, call cyber attacks hazards and use STPA, make security requirements explicit, used at beginning of software development life cycle.
- Identify hazards, then losses. Make model of controller on target. Model is Hacker -> Target, with Activator and Feedback between the two. Sub-hazards of Malware, Attack Types. Hacker -> Target, with Attack and Data between them.
- STPA 17 Cyber Attacks and 50 Mitigations chart. Provides example of combined attack and mitigations.
- Go after big fish first. Know the versions of compilers used by your organization; do they have the latest patch?

- Include network and cyber in stakeholder group. Agile involves it sooner, now involve Cyber sooner.
- Do a lot of research into typical attacks, keep records; there are some attack types unknown.

Questions/Comments:

1. From Jeni – Did you collaborate with Dan Quinlan on cyber work?

   Answer: Yes.

2. From Carol - What is malware definition? How was mitigations determined if hackers wouldn't share attacks?
   Answer: Formal definition in paper. Impede operation, infiltrate. Some malware intentional or bad programming practices.

   From Corina Gonzales – Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to computer system.