

EFCOG SQA Fall 2021 MEETING NOTES

Wednesday November 3, 2021

Quality Moment:

- Christy Renner (PORTS) mentioned the SQA Lessons Learned from ORNL, for the Safety Basis Calculations Assumptions. The periodic review was not part of the annual review. It was suggested for improvements to this review, to bring in SMEs for safety basis calculations. And there is value in performing annual review testing of spreadsheets.

USQ for Safety Software, Presenter Phil Pfeiffer (ANL):

- Phil provided a presentation (see attachments). His presentation title was “USQ Process for Safety Software WRT Software Quality Assurance”.
- The nuclear safety basis analyst completes safety basis documents for Accelerators, Nuclear and Radiological facilities.
- USQ stands for “Unreviewed Safety Question”.
- 10CFR830 has two parts:
 1. Part A & B are for Nuclear Facilities.
 2. Part A is for Radiological Facilities. Less than Haz Cat 3 nuclear facilities.
 3. Part B is only for Nuclear Facilities.
- For federal law, a site is in trouble if the site doesn’t follow 10CFR830.
- Per DOE, USQ is required for each site. The questions and their resolutions are approved by the site office annually.
- USQ looks at accident analysis. The questions are scenarios that could occur for events.
- Consequence analysis result is effect on public, co-located workers close by, and the worker.
- USQ is only for Part B, for nuclear facilities.
 1. Haz Cat 1 nuclear facility, Phil is only aware of one, a Reactor, at ORNL.
 2. Haz Cat 2 nuclear facility, these are less common, only 1 at ANL. Haz Cat 2 affects people at the fence line of the lab.
 3. Haz Cat 3 nuclear facility, these are the most common. Haz Cat 3 affects local co-located people and workers for radiation exposure.
- The USQ process is performed for each building haz cat facility. There are two documents for each facility – Documented Safety Analysis (DSA), and Technical Safety Requirements (TSR).
- USQ can be for any event, software that can occur for the Haz Cat 1, 2 and 3’s. These questions are reviewed.
- There is a non-building nuclear facility for local Transportation within the site, this document is called Transportation Safety Document (TSD). TSRs are for equipment.
- At Argonne, there are There are 7 questions, to determine if positive or negative issue could result. A USQ analysis of an event, can have a positive or negative result. Negative is a good response to USQ question. If you have positive USQ response to question, DOE needs to be involved in resolution of. The USQ process can allow for category exclusions – cat X.
- Many of the sites across the complex use USQ for Safety Software Quality Assurance (SSQA). Phil performed a survey in 2017 and found that 50% of the sites have USQs for their safety software. Many sites do not USQ their safety software. From his survey of sites, he got responses from AMWTP, ANL, CNS, and UDS.
 1. AMWP performs USQ for SSQA in their software change control process.
 2. ANL USQ’s their SSQA. For example, for their radioactive materials inventory, in two applications CURIE site wide, and WMS for waste management facilities.
 3. CNS uses USQ Procedure for SSQA.
 4. UDS USQs their SQAP, SCR, and SRS.
- Phil asked the group how does Argonne fit in with rest of complex? It would be nice to have common procedures for USQ of SSQA.

EFCOG SQA Fall 2021 MEETING NOTES

Wednesday November 3, 2021

- Barbara Hill of ICP provided comments, in January 2022, FLOR AWMP will take over the contract for INL. For the last 5 years, we have not had many positive USQs. AMWP had a positive USQ for Evaluation Safety situation ESS). There is a list of safety basis documents for each facility.
- Carol Olijar of ANL asked what are examples of positive USQ for safety software? An example is database of material on site is found to be incorrect. Add isotope that changes FGE, needs to be passed onto the Safety Basis Group for review the Material At Risk (MAR), which could cause a USQ positive result.
- Carol Olijar of ANL asked Phil as the Software Design Authority for most safety software applications at ANL, does he perform the USQ review in this role? Phil said no, even though he is in safety basis group, he is considered a liaison for SSQA, but for independence another person in the safety basis group performs the USQ review.
- Vicki Pope of LLNL noted her lab has a robust USQ process, anything related to the safety software inventory forms is reviewed. It can take up to a month for USQ to be performed. Vicki suggested Phil place the questions he had for the group regarding USQ for SSQA, at the DOE Forum for Organizational Excellence site.
- Sid Ailes of Atkins Global, asked "How does the USQ process, interface with the PISA process?". For example, at Sid's lab, there was a potential USQ for CFAST, and they needed to re-run fire calculations. Phil answered that PISA is part of USQ.
- Vicki noted that in 2012 CFAST had a PISA at her lab, for the version of software used was not in toolbox. LLNL qualified the new version as a result.
- Phil asked attendees to check with their safety basis people at their sites, to find out what is their labs doing for USQ of safety software. Phil will also post this question at the DOE Organizational Excellence forum, with Carol Olijar's support.

EFCOG SQA Fall 2021 MEETING NOTES

Wednesday November 3, 2021

Panel Discussion #5 Software Spreadsheets Gone Wrong, Moderator Sid Ailes (Atkins Global), Panelists (Barbara Hill, ICP, Christy Renner, PORTS, Carol Olijar, ANL):

- Sid provided a presentation (see attachments). His presentation title was "Spreadsheets Gone Wrong".
- A few organizations have policies for spreadsheets development, such as for templates. Calculation cells are not protected, and the templates are not under configuration control. This can cause problems in the use of the spreadsheet by others.
- A result of the Sarbanes-Oxley Act was for firms to have a better way to manage their spreadsheets. There is a cost of failure of the spreadsheets. Spreadsheets are rife with errors, 88% have mistakes.
- Barbara Hill of ICP had a slide in the presentation deck for Near-Miss Spreadsheets Gone Wrong. Her recommendation is for QA tech and programming to work together on spreadsheets.
- Users often push back, they think of Excel as commercial product, no need to test. But when calculations are wrong, have to find each place that used the calculation. For example, in calculation for waste management, the cause to fix the mistake of the bad calculations cost between 500 an 1 million dollars and caused an extra 2 months to the project. Luckily, they caught the error before sending the waste containers out of the facility. At a laboratory she worked at there was a NCR that was 10 years old for LIMS, having inadequate change control of their testing records which were not kept. It is a simple task to keep records but can be expensive if you don't.
- Another challenge is there are no standards for spreadsheets. NQA-1 does not use the phrase spreadsheet. SQA guide does, the guide can be excluded from a lab's compliance, which can have labs not performing any SSQA for spreadsheets. Look at NQA-1 Subpart 3.2 – 2.7 paragraph 101.1 for reference.
- Calculations can be for input and output. Need to have qualified checker of spreadsheets. NQA-1 allows for hand-calculations. A problem with Excel is it has tools that can make calculations complex, and references to other files. Also, fissile coding FGE can be hard-coded, and at times FGE changes.
- Excel has tools that allow for internal macros, external references, and embedded computer program. For example, GENIE-2000 is for Customized Report Templates, and within this application, there are calculations for Model SCS-Report. The data can be downloaded to Excel for MSTE database. It is important software owners know for commercial packages, what tools are included, otherwise these tools or spreadsheets can sidestep SQA.
- An example is for waste disposal at Environmental Restoration Disposal Facility, there was a spreadsheet to characterize hazardous waste for disposal at ERDF. The calculations in application were for raw NDA data to convert and compare to TRU waste. The spreadsheet was modified by another person than original developer and made waste stream classified for TRU. Waste was buried in drums at 70-foot level. Assumptions were not validated. \$2B error. PAAA can result in Notice of Violation charge.
- The failure modes for spreadsheets are:
 1. No requirements document.
 2. No design document.
 3. No test plans.
 4. No control over changes.
 5. No in-use testing.
 6. No user manual.
- It would be value added to have requirements and tool for spreadsheets. And notification to IT of new spreadsheets. The spreadsheets should follow software life cycle and be included in the software inventory. There should be acceptance testing, authorization of user, user training, and configuration control for changes.
- Barbara suggested adding bullet for retirement plan for spreadsheets. Sometimes when Software Owner retires a spreadsheet, they are not aware others are using it. Software Owners need to know who is using spreadsheets.

EFCOG SQA Fall 2021 MEETING NOTES

Wednesday November 3, 2021

- Veronica Camarillo-Morris of LANL, noted that spreadsheets are everywhere They can be imported and exported in applications. Need to have integrity of data on import. Simple Excel doesn't require SQA. But simple means different things to different people. Research providing to tech aids to run at her lab. How do you delineate what needs to be done for SQA of spreadsheets?
- Christy Renner of PORTS noted don't think of spreadsheet as complicated. Supplier simple spreadsheet calculations went thru engineering, but they missed error after going thru several people. Supplier engineer was junior. Now pipe buried, had to dig up, little calculation, couple thousand dollars problem. Christy used to teach Excel in classroom session. Categorized uses/disabuses of spreadsheets. 9 million spreadsheets at one site. Config manager determined 20 SS spreadsheets, put under control lock-down. The Excel workbook would stop working if someone tried to update it. Recommend creating a decision tree, for what the spreadsheet does. Even simple spreadsheets can have problems.
- Sid noted you can have Excel flat file (only one tab) that may be considered simple, but you still need to document testing for internal macros, references, and databases, imported data, and embedded code is more than simple spreadsheets. Can get a certificate of Compliance Analysis. Can also have multiple instances of spreadsheet. 50 codes calculate repository under conditions, each one of them codes, pre and post processes for the spreadsheets. \$2 million to resolve problem. Important to grill engineers on what using spreadsheet for.
- Veronica noted need to be more cautious. Excel notifications for vulnerabilities, internal. Who is responsible to bring to light to Software Owners? Nightly site updates can make spreadsheets not work. May have configuration management control for any patch for 3rd or 4th digit, to have someone review, for impact on spreadsheets already developed and being used.
- Sid noted at his lab, patch 2 fix for Excel, used by scientist for nanocuries. Scientific notation for Excel can only up to E-14 15 digits, when goes over, Excel does crazy things like truncating. Results don't make sense. Need to validate.
- Barbara added, analysis of changes is important, get software owner involved in this review. Ask question "what could this spreadsheet affect". For engineering, more complicated.
- Sid suggests ask IT group, what precision do they have for security and new software packages.
- Corwin Jones of INL, stated at INL, on network machines, spreadsheets should have SQA, but what about environment not controlled by IT? Can have electronic work packages and calculation on tablet pdfs. Word can have calculations too. Each of these tools use spreadsheets.
- Veronica stated that for safety software, they are not on open business network. Infrastructure controls all software for server. Shareable between groups. Enterprise maintains, for patching to keep up to date. Need to analyze risk.
- Corwin noted for obsolete software, the software is backed up. Patch of new releases of Excel is on current machine. Maintain versions of software.
- Veronica asked, how do you know what everyone is using? How being used.
- Christy responded it would be good to have continual training, as her lab does for SQA. So that site personnel can understand it.
- Theresa Cheek of XXXX, Sid and Christy are knowledgeable around Excel. Need this info shared with the group.
- Sid replied, there is a white paper on firmware. Example of this is key fireman puts into panel to have access to building/room. The panel uses an software interface.
- Vicki noted at the EFCOG website for SQA there is White Paper entitled "WP 2019 SQA Firmware". She placed the link to it in chat, it is copied here.

EFCOG SQA Fall 2021 MEETING NOTES

Wednesday November 3, 2021

- Sid went over the questions the panel came up with:
 1. Who should be involved in spreadsheet? Tech & QA people.
 2. When spreadsheets retire, should there be formal process? Yes, need to look for others who use spreadsheets. All codes.
 3. What happens when spreadsheet fails? Analyze, run report old and new way, what changed. There can be challenges when people copy/paste. 1 error can affect many calculations. Perform Extent of Condition (EOC).
 4. Should testing be independent? Yes. That's the best we could do. Need to evaluate errors. Christy noted developer will see same thing every time they review. Independence is a plus.
 5. Why is it necessary for IT or QA to be involved? Definition of "Like for Like" may be different.
 6. What about copy mistakes, dragging a copy of formula? You may have finding for NDA, for adding extra digit on number. All spreadsheets' formulas should be locked down. Encourage people to try to break spreadsheet in testing. Use different data. Perform hazard analysis on formulas. When spreadsheet is locked down, only people who use spreadsheet should have access to it, all performing the same calculations. Have someone else validate your spreadsheet. Ellen Clark at PORTS came up with spreadsheet training and auditing using IEEE documents.
- Barbara suggested having metrics with spreadsheets.
- Christy suggested for Waste spreadsheets lock them down if used for characterization. Perform through design, and configuration management.
- Sid added, engineers re-use same spreadsheet. Require multi-use spreadsheets under configuration control.
- Teri Vincent of CNS/Y-12 & Pantex, asked "What is timing for Sid's paper?". It would be good if we could have it done. Sid responded he is getting started on it, should be ready next year.
- Sid noted the Genie 2000 issue was caught by engineer buried in back of user manual.
- Marlene Underwood of PORTS, Could independence be based upon risk level? What about spreadsheet template? Could have tab for change control, and overview tab, naming conventions for variables. Sometime issues occur when exporting from SharePoint to Excel.
- Christy noted NQA-1 requires independence in testing. How much independence depends upon working with Software Owner and developer.
- Marlene noted, for non-safety software, there is a low-level risk, SQA may not be necessary.
- Barbara stated, always ask question "What is worst thing that can happen?" in discussion with software owner.
- Sid added, for design verification, do not need to be expert. If safety related, you may want person with multiple disciplines.
- Greg Pope of LLNL, added there is a Spreadsheet Testing Sub-group in SQA he is the leader for. He and the group are working on testing checklist, he would like to get this checklist in hands of people.
- Barbara noted for this sub-group, there was Pilot that had useful questions.
- Greg added it is important to evaluate number of testing tools. Problems can be easily found for low hanging fruits using these tools. Need automated tool for testing.
- Sid & Greg noted, others could participate in task group. Look at design flaws. Tool could record testing done.
- Greg mentioned that Microsoft would not put out Excel with different answers in later versions. The most current Excel version is backward compatible.
- Christy has old version of what her lab used for testing of spreadsheets; she will check into to see if it can be shared.
- Greg noted please be careful with passwords for spreadsheets. No way to recover lost password in Excel.
- Theresa Cheek of XXX, asked could the talking points of white paper come out before task completed in group?
- Vicki responded presentations will be available at EFCOG website. The checklist Greg is working on, will be available prior to white paper.

EFCOG SQA Fall 2021 MEETING NOTES

Wednesday November 3, 2021

Other Group Issues, Moderator Vicki Pope (LLNL).

- Vicki mentioned that her Leadership Role of this group as Chair, she wants to step down in next couple months, around January. Vicki has been the Chair of this group for 5 years. There is a document that describes the leadership roles duties at the EFCOG website, and EFCOG SQA box folder. Vicki would like to have nominations and voting in December. It is a great opportunity, good people to work with. Vicki provided the link to the EFCOG SQA Leadership Duties document in the chat.

Sub-task Group Introductions, Sub-task Group Leaders.

- Task group leaders went over what they want to accomplish in their breakout sessions at this meeting.
 1. Christy Renner of PORTS, leader for SW Standards Matrix Sub-task, noted that the current workbook for her task is at the Box site. The workbook includes orders, and policies that affect SQA with tabs for each one. Added IEEE Carnegie Mellon CBOC DOT, and NASA documents. Included NIST standard 800-53, sharing with assessments. To find this workbook at Box, go to T7 Software Standards & Orders-> document for 7.13 Orders and Policies Affecting Software. There is a Summary Listing of tabs. This document will be maintained. Getting started on white paper. Get input from group. Teri Vincent is working on white paper with Christy.
 - Donna Riggs of Riggs Consulting, asked what is intent of White Paper? Christy responded there is a EFCOG document for way to do White Paper. Maybe White Paper is not needed.
 - Vicki responded, could have white paper introduction of workbook. Also, how to navigate. This document can be a couple pages in length.
 - Donna noted, welcome to add this info to the workbook. Any input is welcome.
 - Pat Auer of LLNL, noted this white paper would be similar to what was done for Suppliers white paper.
 - Vicki noted can have white paper cover attached to workbook.
 2. Pat Auer of LLNL, leader for Toolbox Alternative Sub-task, provided overview of his group. Started on this task in April, looking at how to store codes, guessing at answers. DNSFB is looking into Toolbox. Not getting answers back yet on update of survey task from AU-32 Chris. Talk about option of using supplier modal. Stuck on expanding list for RSICC codes, for criticality safety codes.
 3. Greg Pope of LLNL, leader for Testing Spreadsheets Sub-Task, noted that his group is talking about challenges with spreadsheets, such as used for scientific calculations. Writing white paper and developing checklist to test spreadsheets. Also looked at automation tools. Work on pilot of checklist to send out with minutes of this meeting to review by group.

Sub-task Breakout Session #1, Sub-task Group Leaders & their groups.

- Each of the Sub-Group Leaders may have taken notes of their sessions. No notes were taken by secretary.