USQ Process for Safety Software WRT Software Quality Assurance

Phil Pfeiffer

Argonne National Laboratory

ISM & QA Working Groups 2021 Fall Meeting

November 3rd, 2021

GOAL was to Collect Information from DOE Labs:

- Basically, ask the questions on:
  - Current Practice in DOE Approved) USQ Process (locally by Site Office)
    - NOTE: This is different for each SITE (allowed per 10 CFr 830 Part B)
    - Part B is specifically Nuclear Facilities
      - Hazard Category 1 (not common)
      - Hazard Category 2 (somewhat common)
      - Hazard Category 3 (very common)
- Argonne: Nuclear and Waste Management Division
      - Hazard Category 2 (one facility)
      - Hazard Category 3 (two facilities)
      - TSD (Transportation Safety document)
      - Various Radiological Nuclear Facilities, i.e., less than HC-3
        - NOTE: 10 CFR 830 applies, however only Part A applies (QA), Part B NOT required (USQ implications)

Input from the following DOE Labs:

- AMWTP: Advanced Mixed Waste Treatment Project
  - DOE Idaho Operations Office EM
- Argonne: Nuclear and Waste Management Division
  - DOE-Argonne Site Office (ASO)
- CNS: Consolidated Nuclear Security, LLC, Y-12
  - DOE-Oak Ridge National Laboratory (ORNL)
- UDS: Uranium Disposition Service, LLC - AREVA
  - DOE Richland Operations Office

AMWTP

1. *Change control process documentation.* Any documentation that is used to implement an AMWTP change control process. Examples of this documentation include but are not limited to: Document Change Requests, Facility Modification Proposals, Software Change Requests, or Software Data Change Requests.
2. *Minor changes to nuclear related software.* Changes made to nuclear related software (including software generated queries/reports) that cannot affect the acquisition, derivation, storage, transfer, reference, comparison, tracking, or manipulation of FGE data. In addition, the software change cannot allow any SSC to be operated outside normal operating conditions and/or parameters.
3. *Proposed change.* Any alteration or addition, temporary or permanent, to the facility configuration, facility documentation, design requirements, specification, facility software, procedures or processes, or the conduct of tests or experiments not described in the hazard analysis. Proposed changes are evaluated to determine if DOE approval is required. A change to a structure, system, or component alters its: (a) function(s), (b) the method of performing the function(s), or (c) its design configuration. Identical replacements or approved equivalent parts are not changes.

AMWTP (continued)

4. Minor Changes to Nuclear Related Software (Use of Cat. Exclusion or USQD)

   The application of this categorical exclusion shall be applied by a qualified USQ evaluator. For this categorical exclusion to apply, the proposed software change must meet the definition of a minor change to nuclear related software as provided in MP-NSPC-3.2. If the change affects FGE data in any way, or if the change causes any SSC to be operated outside normal operating conditions and/or parameters, either temporarily or permanently, then this categorical exclusion cannot be applied and a USQ Determination must be completed. A software change that restores an SSC back to its designed functionality is not a change that causes the SSC to be operated outside normal operating conditions or parameters.

Argonne

- Purpose is to discuss the reason for USQ review of safety software, criteria to apply, and then the appropriate procedure to place the requirement.
- 10CFR830 - USQ definition
  (1) The probability of the occurrence or the consequences of an accident or the **malfunction of equipment important to safety** previously evaluated in the documented safety analysis could be increased;
  (2) The possibility of an accident or malfunction of a different type than any evaluated previously in the documented safety analysis could be created;
  (3) A margin of safety could be reduced; or
  (4) The documented safety analysis may not be bounding or may be otherwise inadequate.
- 10CFR830 - USQ process must be implemented in situations where there is a:
  (1) Temporary or permanent **change in the facility** as described in the existing documented safety analysis;
  (2) Temporary or permanent change in the procedures as described in the existing documented safety analysis;
  (3) Test or experiment not described in the existing documented safety analysis; or
  (4) Potential inadequacy of the documented safety analysis because the analysis potentially may not be bounding or may be otherwise inadequate.

Argonne (continued)

- CM-102 Procedure – USQ Procedure
  - **Change:** A structure, system, or component (**SSC**) is considered to be changed if any of the following are altered:
    (1) the **function**(s),
    (2) the method of accomplishing those functions, or
  - (3) the physical configuration of the item.
  - **Equipment important to safety:**
  - For the purposes of this procedure, equipment important to safety includes any equipment whose function (including malfunction or failure) can affect safety either directly or indirectly. This includes safety-class SSCs; **safety-significant SSCs**; **supporting SSCs** to safety systems that are **required for the safety function**; other systems that perform an important defense-in-depth function; equipment relied on for safe shutdown; and in some cases, process equipment.
- USQ applicability – changes to SSCs – changes to Safety Software that performs a safety function specifically credited in the TSR or hazard analysis tables in Chapter 3 of DSA.
  - Evaluate – could a change to the software directly cause a condition that is outside the safety basis, unevaluated, or non-conservative with respect to the TSR controls; thus requiring DOE approval.

CNS

1. USQ process has an exemption in their DOE approved USQ Procedure for changes made by the vendor of software that complies with our SQA procedure.
2. Triggers are present within procedures that direct application of the USQ Process in situations where we have determined it is required.

UDS

- Applicability of the USQ Review Process to the Software Quality Assurance Documents
  - USQ review process for Software Quality Assurance documents developed in accordance with UDS-U-PEP-0018, *Design and Process System Software Quality Assurance*.
  - The conclusion is that 3 (three) types of documents (SQAP, SCR and SRS) **DO** require USQ review
    - SQAP: Software Quality Assurance Plan
    - SCR: Software Change Request
    - SRS: Software Requirements Specification

UDS (continued)

- All other types of software QA documents reviewed **DO NOT** require the USQ review process.
    - SFD: Software Functional Description
    - SRER: Software Risk Evaluation Report
    - SIC: Software Installation and Checkout
    - SID: Software Implementation Documentation
    - SVVR: Software Verification and Validation Report
    - SVVP: Software Verification and Validation Plan
    - SSAR: Software Safety Analysis Report
    - SUM: Software User Manual
    - SCD: Software Classification Documentation

Questions and Discussions

- Generally, 10 CFR 830 drives the need for the USQ Process
  - Nuclear Facilities (HC-1, 2, 3 and TSD) must be evaluated via the USQ Process
  - Radiological Facilities (less than HC-3, only Part A of 10 CFR 830 (part A only, which involves the Quality Assurance requirements)
- ?
- ?
- ?