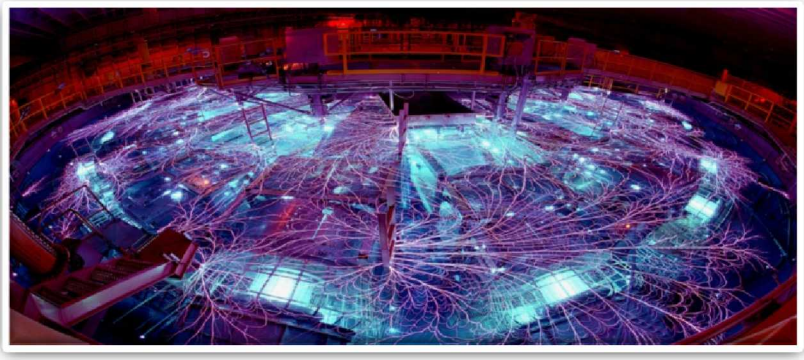
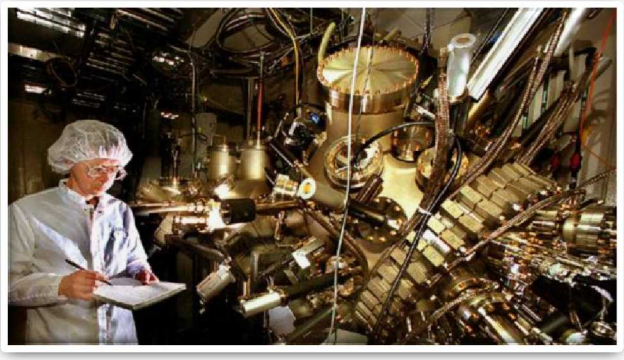
Exceptional service in the national interest

SAND2012-3477C

Sandia National Laboratories





Electronic Unreviewed Safety Question (eUSQ) System Lessons Learned

U.S. DEPARTMENT OF ENERGY | NNSA

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Lessons Learned Topics

Sandia National Laboratories

- Purpose of eUSQ
- eUSQ Features
- Lessons Learned 1 – Software Documentation
- Lessons Learned 2 – Developing an Automated Process
- Lessons Learned 3 – Effect of Code Changes
- Conclusions

Purpose of eUSQ

Sandia National Laboratories

- Developed to automate the SNL Unreviewed Safety Question process.
  - Used to enter, store, process, and access USQ form entries.
  - Augments, does not replace, the current USQ process.
  - Intended to reduce manual effort, not mental effort.
  - Reduces opportunity for human error through well-defined logic restraints, roles, and responsibilities.
  - End result (document) is identical to approved form.
- Automatically ensures proper record retention.

eUSQ Features

Sandia National Laboratories

- Uses electronic signatures.
- Auto-email to users for workflow actions.
- Safety basis document references pre-loaded for each facility in USQD worksheet.
- Ability to attach files to any USQ document.
- Copy, revise, and cancel capability for existing entries.
- DSA page change checkbox allows users to track entries that may have impact to their DSA to assist in annual update process.

Lessons Learned 1 – Documentation

Sandia National Laboratories

- Lessons Learned: Providing a level of software documentation commensurate with the level of risk associated with failure of the software will save time and effort during the software lifecycle.
  - Initially believed that a requirements document was sufficient
  - Research into what was being performed elsewhere at SNL
    - What were larger software projects doing
    - Corporate processes for software quality assurance
  - Concluded that more documentation was beneficial
  - Reduction in cost of re-engineering software and software maintenance throughout the software lifecycle.

Lessons Learned 1 - Documentation

- Sources used to develop eUSQ documentation:
  - External requirements:
    - 10 CFR 830, Nuclear Safety Management, Subparts A & B
    - DOE Order 414.1C, Quality Assurance
    - NQA-1-2000, Quality Assurance Requirements for Nuclear Facility Applications
  - Sandia Corporate QA and Software Processes
    - Graded approach based on risk/consequences of software failure
    - Determination of Safety Software
  - Format and content for eUSQ documentation was taken from IEEE software standards, where appropriate
  - SNL USQ Procedure

Lessons Learned 1 - Documentation

Sandia National Laboratories

- Resulting Documentation
  - Software Design Document: Sufficiently describe the eUSQ system such that another application developer with the proper skills would be able to support the software product lifecycle.
  - Software Requirements Specification (IEEE Std 830-1998): Defines the software requirements necessary to meet procedural/USQ process requirements, and to provide the proper controls for security, document control/retention, and usability.

Lessons Learned 1 - Documentation

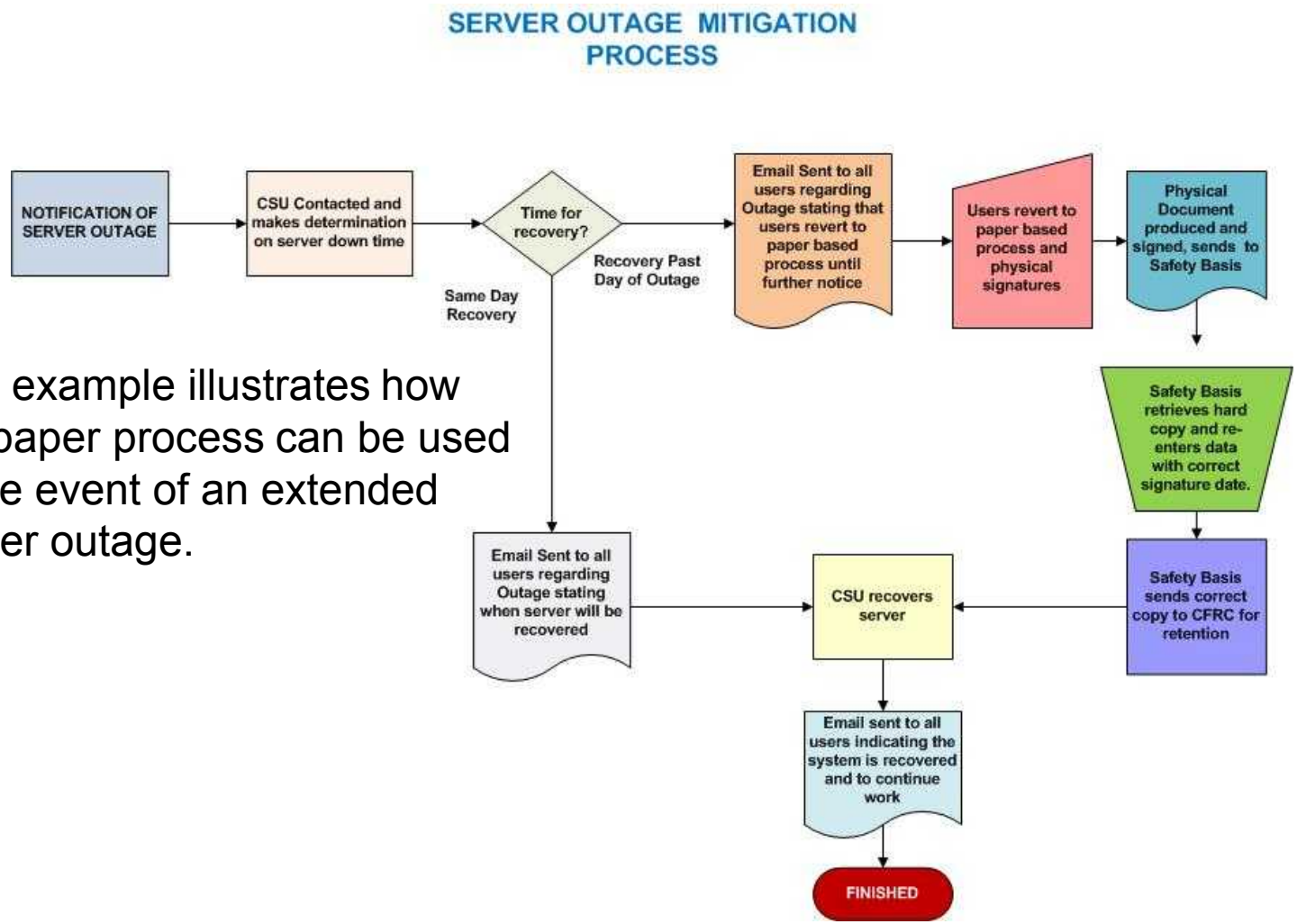
- Resulting Documentation (continued)
  - Test Plan (IEEE Std 829-1998): Identify tests necessary to verify that the requirements from the requirements documents were achieved.
  - Practice Level and Safety Software Determination: Identify the magnitude of risk associated with a potential failure of the eUSQ software. Used to determine graded approach to eUSQ development and lifecycle maintenance.

Lessons Learned 1 - Documentation

- Resulting Documentation (continued)
  - Software V&V Plan*: Document the level of verification and validation required for eUSQ based on application of the graded approach to software quality.
  - Risk Mitigation Plan: Identify potential problems before they occur such that risk-handling activities could be planned and invoked as needed.

* Formal V&V was not required for the eUSQ System.

Example - Risk Mitigation Process



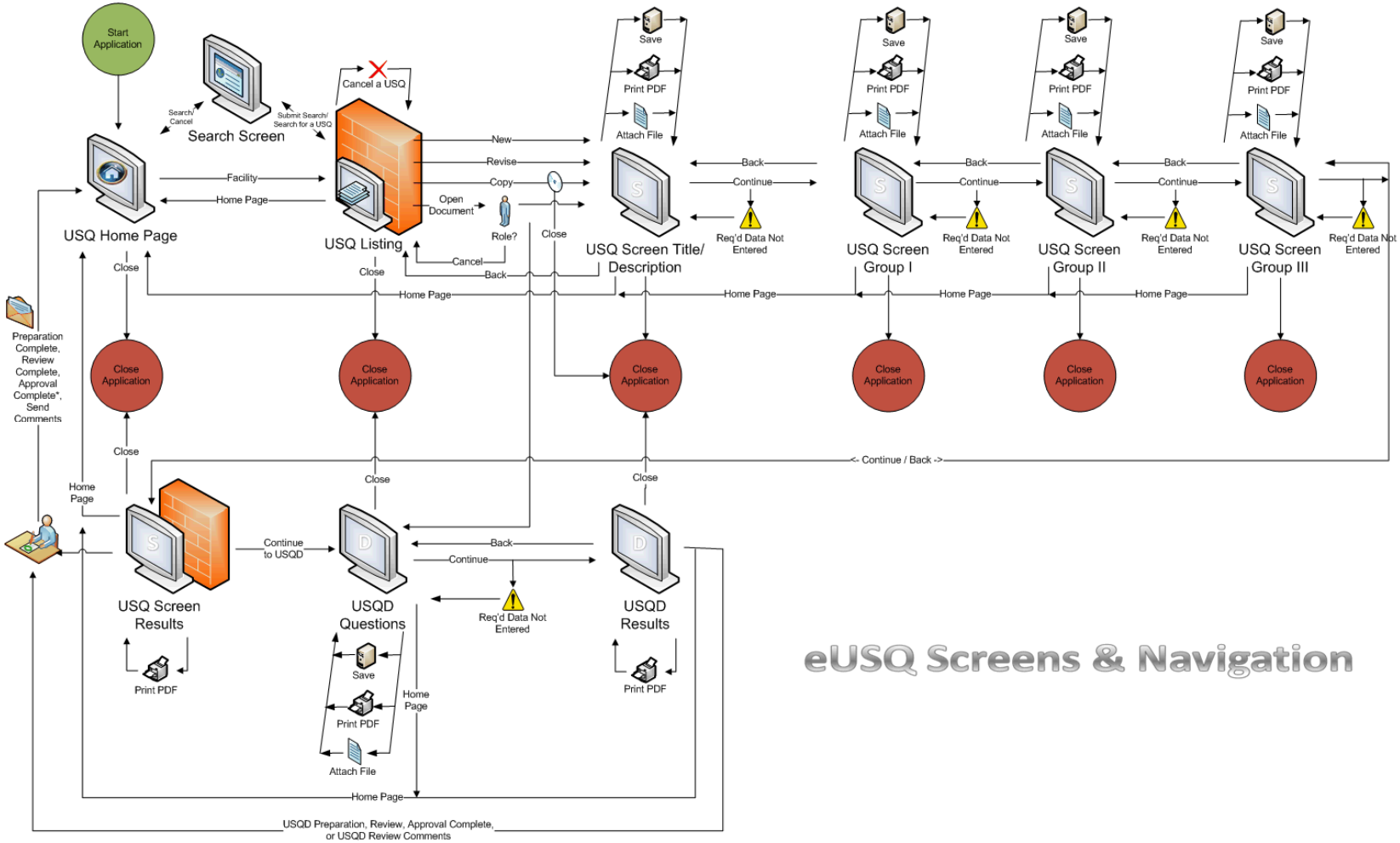
This example illustrates how the paper process can be used in the event of an extended server outage.

Lessons Learned 1 - Documentation

Sandia National Laboratories

- Resulting Documentation (continued)
  - Software Lifecycle Process (IEEE Std 11207-2008): Provides information on the implementation and tools used in the software product lifecycle and version updates for the eUSQ system.
  - Diagrams were developed to facilitate development, ensure software consistency (e.g., consistent options and navigation), and enhance usability.

Example – Navigation Diagram

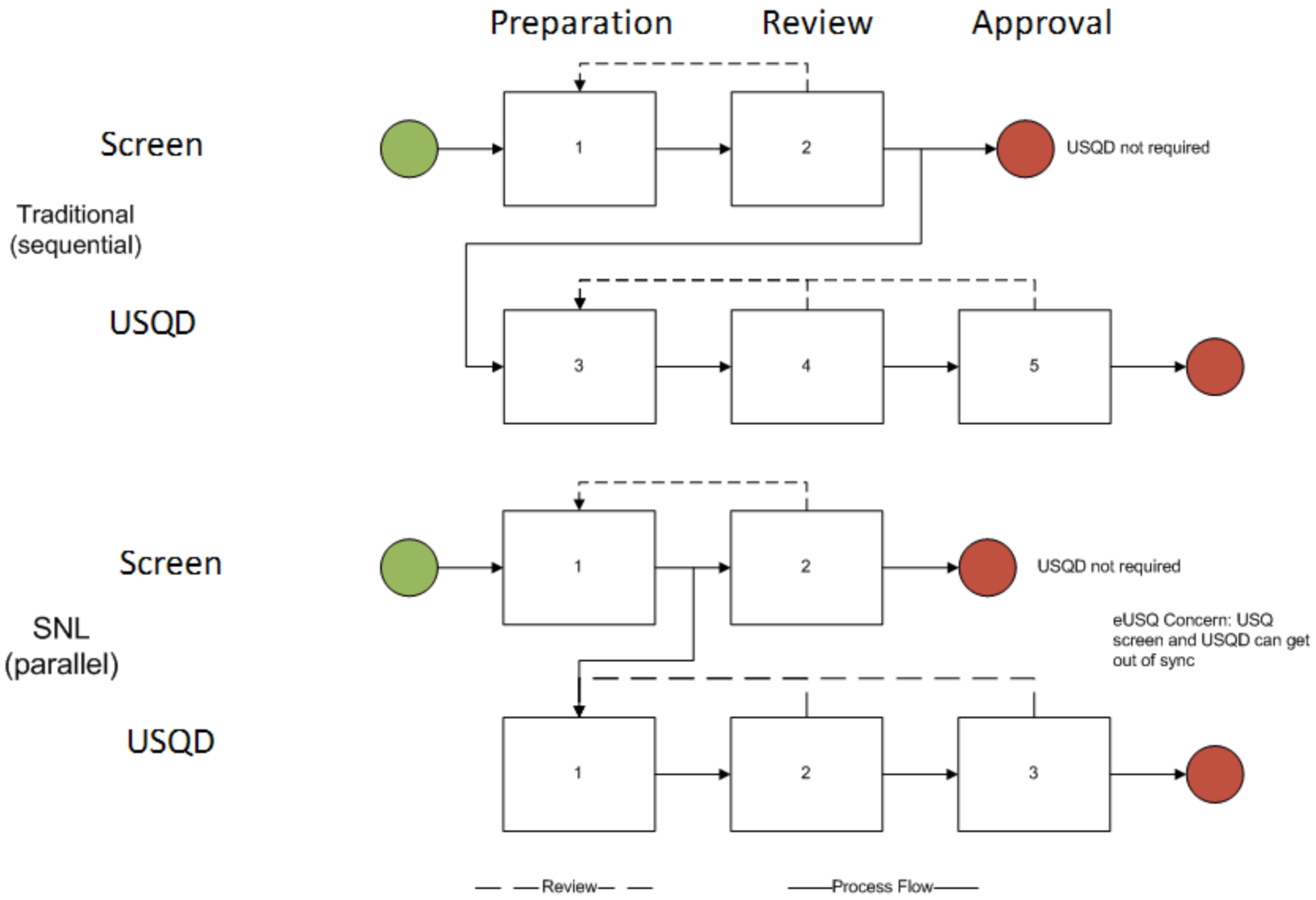


eUSQ Screens & Navigation

Lessons Learned 2 – Developing an Automated Process

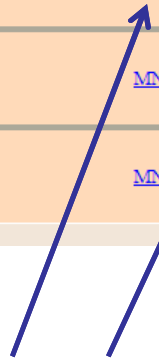
- Lesson Learned: Simply process when possible.
  - Paper process believed to be very simple.
  - Processes for the two USQ forms (screening checklist and USQD) documented separately in two flow charts.
  - Difficulties associated with two forms
    - What was considered a record (e.g., completed screening checklist that didn't require a USQD).
    - When to create (or remove) the USQD record.
    - How to list the documents and store in the database (one record vs two).
    - How far a USQD could go through review and approval process prior to completing a review for the screening checklist (based on how the paper process had been used).

Completion Process of Screen/USQD



Screen/USQD Listing

USQ(S/D) Number	Title	Status	Date Started	Prepare
MNF-11-0013D-R0	Implement DOE O 426.2, Personnel Selection, Training, Qualification, & Certification Requirements...	Approved	08/11/2011	Martin-Mil
MNF-11-0013D-R1	Implement DOE O 426.2, Personnel Selection, Training, Qualification, & Certification Requirements...	Approved	08/29/2011	Martin-Mil
MNF-11-0013S-R0	Implement DOE O 426.2, Personnel Selection, Training, Qualification, & Certification Requirements...	Reviewed	06/16/2011	Martin-Mil
MNF-11-0013S-R1	Implement DOE O 426.2, Personnel Selection, Training, Qualification, & Certification Requirements...	Reviewed	08/29/2011	Martin-Mil



These two items are part of the same evaluation (S after sequence number = screening checklist, D = USQD). While they may be easy to identify (and distinguish them from the Rev. 0 version) in this short list, misidentification might be an issue on a large list. This has not yet been identified as an issue or concern by any of the end users.

Lessons Learned 2 – Developing an Automated Process

- While revising USQ procedure to incorporate guidance from DOE G 414.2-1B, simplifying process by combining two forms into one single form.
  - Will require a single set of signatures; one document to submit for record retention.
  - Will be listed once on the listing (status) page.
  - Reduces code complexity to search and connect two database records (specially when applying multiple Boolean fields).
  - Complexity of code to handle transition from screening checklist to USQD greatly reduced (process will become linear).

Lessons Learned 3 – Effect of Code Changes

Sandia National Laboratories

- Lesson Learned: Document software flow and assumptions that are made during development to minimize impact of adding new features or code changes.
  - Assumptions or decisions are often made concerning automation of process details that are not detailed in existing procedures.
  - Code changes can have unintended effects on the these assumptions.
  - Use the test plan to verify code changes do not impact functionality of the existing code.

Lessons Learned 3 – Effect of Code Changes

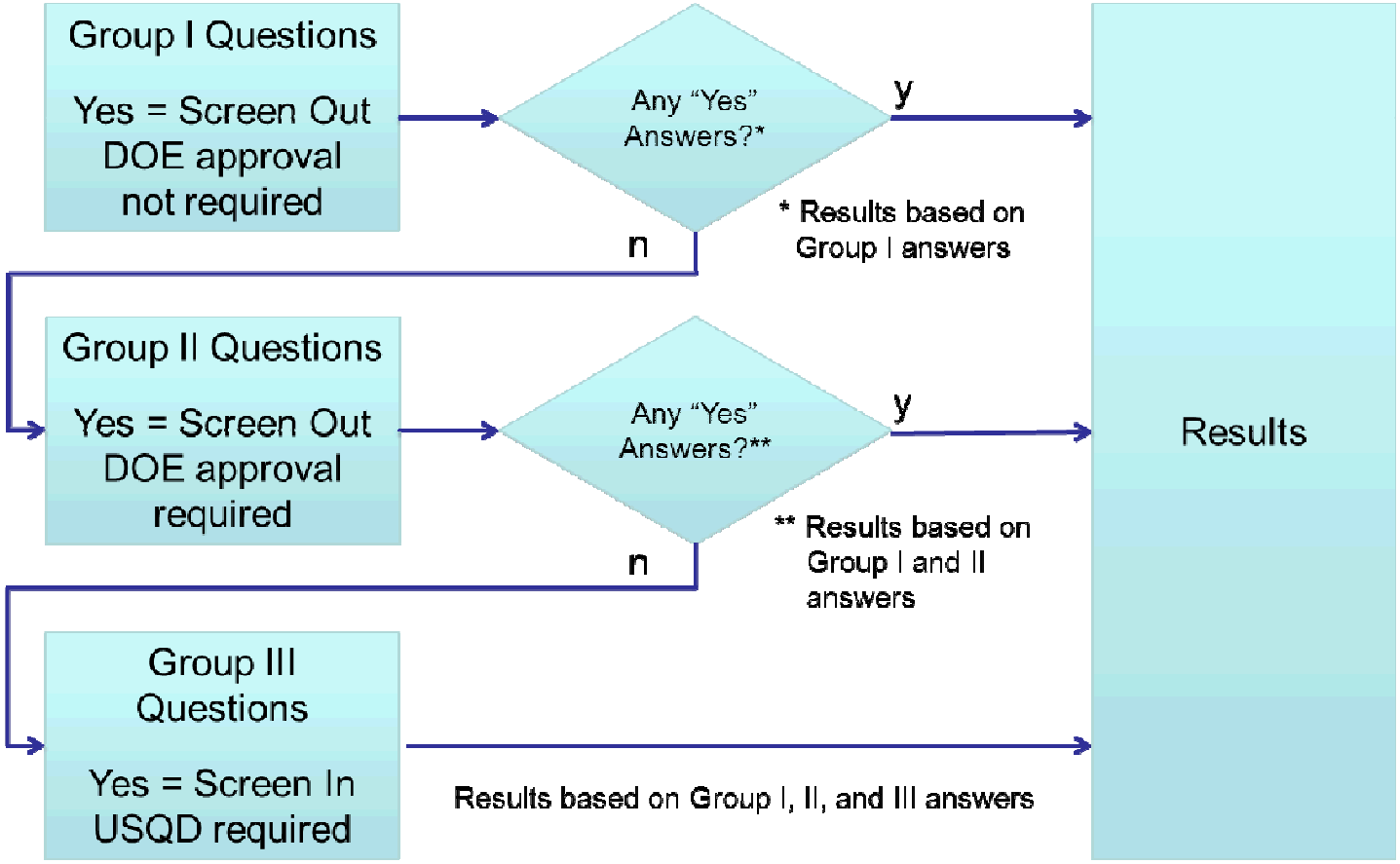
Sandia National Laboratories

- eUSQ Example – Timeline of Events:
  - eUSQ initially developed without features to copy or revise evaluations.
  - Initial code assumed that information was entered only once (i.e., no information has yet been entered for subsequent parts of the screening checklist). This assumption was consistent with the directions provided on the paper form.
  - Copy/revise features added.
  - Requirement clarification: Draft screening checklist must identify results after any questions have been answered (previously results were not identified until form was completed).
  - eUSQ code updated, using same assumption as before.

Lessons Learned 3 – Effect of New Features

Sandia National Laboratories

eUSQ Evaluation of Screening Checklist Results



Lessons Learned 3 – Effect of New Features

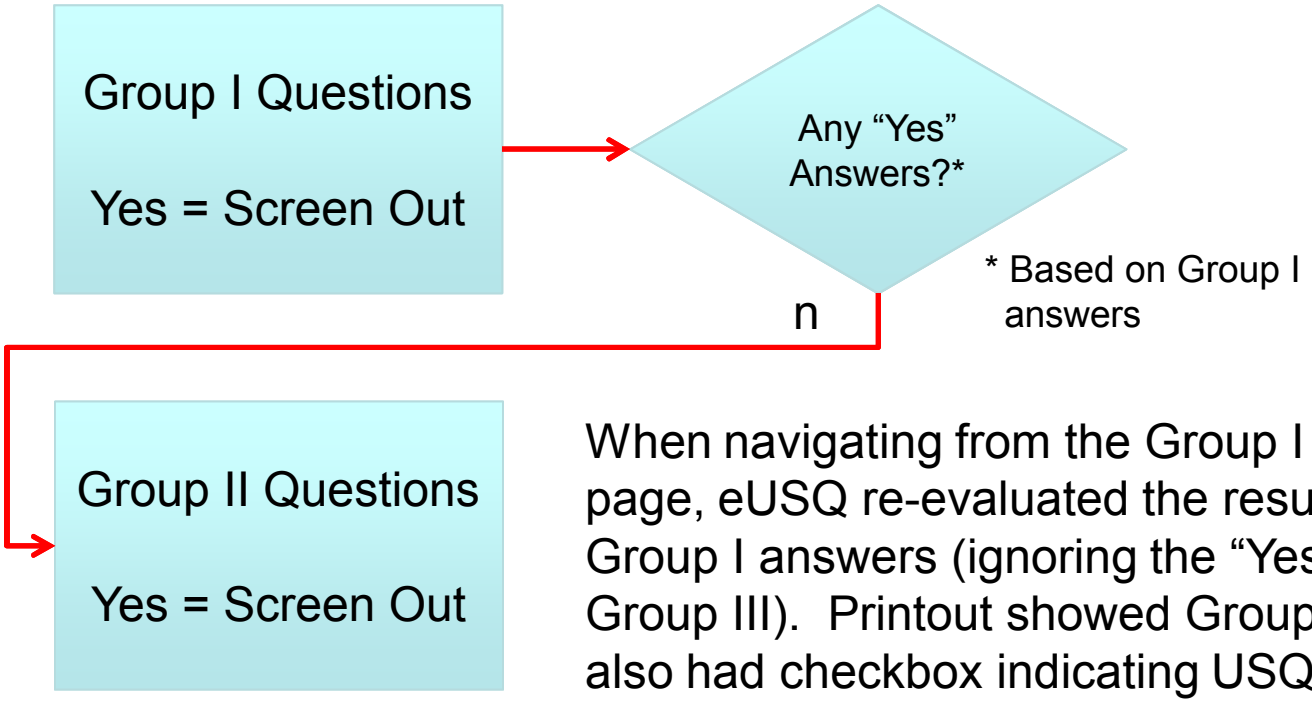
Sandia National Laboratories

- Timeline of Events (continued):
  - After implementing the updated code, an end user identified that incorrect results started appearing on the draft screening checklist.
  - The draft results were inconsistent; at times the results were incorrect while at other times the results were correct.
  - Results of completed/signed screening checklist were always correct.
  - Tests were performed, re-creating the conditions the end user provided.

Lessons Learned 3 – Effect of New Features

Test – Copy a previously performed screening checklist/USQD. Without changing any data, navigate to the Group II Questions. Print a draft PDF of the screening checklist. Verify screening checklist results accurately reflect the answers to the questions.

Test Data - The previous evaluation had “No” answers for the Group I and II questions, and a “Yes” answer for a Group III question.



When navigating from the Group I page to the Group II page, eUSQ re-evaluated the results based on only the Group I answers (ignoring the “Yes” answer in Group III). Printout showed Group III “Yes” answer, but also had checkbox indicating USQD was not required.

Conclusions

Sandia National Laboratories

- Simple processes such as the USQ process can become complex for automation.
- Lessons learned illustrate the difficulty to preclude problems that will occur during software development and maintenance.
- Additional documentation will reduce (but not preclude) additional effort of re-engineering or significant impact to the end user during the software lifecycle resulting in an overall cost savings.
- Communication of these lessons learned should help to provide additional thought for those who will be implementing their USQ or similar process in the future.