



DOE Standard 3007

Update 24 January, 2007



Briefing Goals

- 3007 issuance status
- Response to previous Clarification Questions
- Refine remaining Clarification Questions

Standard 3007 Approval Status

- In the works for two years.
- Inputs received from
 - NCS Managers End User Group
 - EFCOG SAWG
 - Criticality Safety Support Group
 - Criticality Safety Coordinating Team
 - DNFSB
- All RevCom DOE/NNSA comments dispositioned. Verifying DNFSB comments dispositioned.
- Will be issued shortly.

Clarification to Items Submitted

1. Question. Page 5, Section E, Process Analysis & Page 10, Section A, 2nd paragraph. This section seems to be inconsistent with DOE Guide 421.1-1. DOE Good Practices Guide – Criticality Safety Good Practices Program Guide for DOE Nonreactor Nuclear Facilities regarding expectations for criticality safety/frequency. Clearly, the stated goal in the proposed DOE-STD-3007 of $1.0E-04$ per year or less is different than the stated goal of $1.0E-03$ per year or less in DOE Guide 421.1-1. Which goal is correct? This would seem to be a new expectation.

1. Response.


References to numeric risk values will be stricken from 3007 to meet a DNFSB comment. The following sentence from section E will be deleted: This section should document the fact that the controls are adequate to allow the risk of a criticality accident to be considered at least extremely unlikely. Also, the following sentence from section A, page 10 will be deleted: A CSE showing that a process is double contingent typically demonstrates that the frequency of a criticality accident is less than or equal to one in 10,000 years (i.e., in the extremely unlikely range).

2. Definition of Unlikely. The first sentence uses the term improbable, thus implying probability. The second sentence uses frequency. Which is correct?


- ***Both. No changes expected.***

(The second sentence states that an unlikely event is not expected to occur more than once in the lifetime of the facility. If expected facility life is 50 years, then this is not consistent with the third sentence that states that an unlikely events are expected to occur with a frequency less than once in a hundred years. Again, which is correct? The last sentence, “Due to the general lack of statistically reliable data, assigning numerical probabilities to events is not usually justifiable and when used should be backed up with references.” This philosophy/concept (probabilities not reliable) is not consistent with the use of PRA in the Commercial Nuclear Industry. However, I agree that when specific probabilities are used, the source should be referenced. Does this last sentence really add value to the definition of “Unlikely”?)

- More in question 9




3. Question. Page 10, Section A, Documenting That A Criticality Accident Is Not Credible, 3rd paragraph. The previous version contained the following words regarding incredible scenarios discussions. “A much higher standard for control selection than is acceptable for documenting adherence to the double contingency principle is required in this instance.” This certainly makes sense. The current version contains the statement. A CSE showing that the nature of the process precludes the potential for a criticality accident or that a criticality accident is not credible or not physically possible should not rely on simplistic formulas for the number of controls or contingencies in place (i.e., by defining not credible as equivalent to three concurrent contingencies or concurrent failure of four controls, etc.).



3 (response) Don't read more into this than is there. It simply means that arbitrarily defining 3 to 4 controls as getting you to "not credible" is not going to meet the burden of proof required in this instance. It means that a more formal basis needs to be developed and defended.

4. Question. Page 11, Section B, Need for Criticality Alarm Systems. Section 4.1.1 of the Standard contains the following statement. "Installation of an alarm system implies a nontrivial risk of criticality." I'm looking for guidance regarding the terms "credible" and "nontrivial" risk. Is the assessment of credible or nontrivial risk made assuming a) absolutely no controls are required (nature of process or segmentation only) for the criticality analyst to conclude that criticality is not credible, b) some reasonable number of controls and/or programs for a few scenarios are required for the criticality analyst to conclude that a criticality is not credible, or c) a significant number of controls and programs are required for almost all scenarios in the NCSE for the criticality analyst to conclude that the frequency with controls/programs is not credible? My thought would be "b" simply because I think "a" and "c" represent unreasonable extremes, but would appreciate your thoughts.



4. Response. ***No burden of proof was discussed during the writing phase of 3007. However, option (b) as stated seems reasonable as long as appropriate DSA/TSR level control result from relying on them to absolutely prevent a criticality accident.***

5. Is it permissible to arrange the CSE differently (for example, eliminate the “Introduction” and “Methodology and Validation” sections) as long as the content of those sections is included elsewhere and still meet the Standard?

1.2. DOE O 420.1B, Attachment 2, Section III 3 b (5) requires performance of CSEs in accordance with DOE-STD-3007-1993 or successor document unless approved by DOE. If deviation from the format is not allowed, at what level of DOE is approval to use a different format approved (local site office or headquarters)?


- As worded, 3007 does not permit a format other than that specified.***

6. A contingency seems to be defined as a parameter change as opposed to an event and compliance with the DCP tied to demonstrating that "...at least two unlikely, independent, and concurrent changes in ... parameters must occur before a criticality accident is possible." (DOE-STD-3007-YR TBD, section II E) Is it permissible to define contingency as the event leading to parameter change(s) as long as the impact of the event on nuclear-related parameters is identified and evaluated and still meet the Standard?

- Yes. "Events" are initiators that potentially lead to contingent changes in process parameters. The parameters are controlled, not necessarily the initiating events.***


7. ANSI/ANS 8.1 allows control of a single parameter (section 4.2: “Nuclear criticality safety is achieved by controlling one or more parameters...” (emphasis added)) and also provides various single parameter limits. Requiring adherence to the DCP (DOE O 420.1B, Attachment 2, Section III 3 b (4)) and defining the DCP in terms of “at least two parameters” appears to prohibit this without documenting, justifying, and obtaining DOE approval. Is this the intent of the Standard?

- ***When a criticality accident is credible, single parameter control does NOT meet DCP as intended by ANSI/ANS-8.1.***



8. If single parameter control is not allowed, at what level of DOE is approval to use single parameter control approved (local site office or headquarters)?

- ***Front matter to 420.1B assigns approval of single contingent operations to the PSO. The PSO's can delegate to site office managers but it is at the discretion of the PSO.***




9. Contingencies and controls are tied to a frequency through the new definition of unlikely (“...not expected to occur in the lifetime of a facility....expected to occur with a frequency less than once in a hundred years...” (DOE-STD-3007-YR TBD, Definitions)). Contingencies are not expected to occur and controls are not expected to fail within the time period established by the definition.

Three related questions.

9.a. It is difficult to conceive of an administrative control that would be robust enough to never fail over the facility life or for 100 years. Almost all administrative controls and contingencies related to failure of the controls would be precluded by this definition. It would appear that the only way to utilize an administrative control would be to have at least two in place and claim that failure of both concurrently would not occur. Is it the intent of the Standard to require multiple administrative controls?

- ***Do not confuse failure of controls with the occurrence of the contingent event. An unlikely change in process conditions (i.e. parameter) should not occur more than once in the lifetime of the facility or more than once in a hundred years. How often does full flooding occur? How often does something exceed a double batched mass?***



9.b. If it is not the intent to require layered administrative controls, what would be an acceptable rationale for claiming that an administrative control will not fail over the facility life or for 100 years?


Layered controls are intended.

9.c. While more reliable than administrative controls, design features, particularly active ones, suffer from a similar problem. Does this mean that we have to assign failure frequencies/probabilities to design feature controls? If probability is not intended, what is required to meet?

- ***No. 3007 never requires control failure frequencies to be quantified. A sound qualitative argument should be made as to why the contingent event (i.e. unlikely change in process parameters = unlikely change in process conditions) meets the expectations of being unlikely.***


10. Among the evaluation criteria to be used to select controls for inclusion in the DSA/TSR is “....The minimum set of controls selected for inclusion should be those that meet the following conditions: (B) loss of control could result in a singly contingent condition” (DOE-STD-3007-YR TBD, section IV, criterion 6). Most CSEs demonstrate that worst case (from NCS perspective) normal conditions are subcritical and then, starting from the worst case normal, that credible abnormal conditions are also subcritical. The loss of a credited design feature is often considered as one of the “abnormal conditions” and shown to result in a subcritical configuration. Is the criterion above intended to require that the control be part of the “minimum set” unless it can be demonstrated that, starting from the already abnormal condition, any second failure can also be shown to result in a subcritical configuration (essentially requiring triple contingency or listing the design feature in the DSA/TSR)?

No.




11. Is the intent that the evaluation to determine if a loss of control could result in a singly contingent condition or not be rigorously documented for each and every control?


No.



12. Question. The CCR is described as a technical reference to the DSA which facilitates identification of commonly important controls. This approach can easily lead to “generic” controls that are applicable for multiple processes such as use of fixed spacing, safe container dimensions/volume, drainage features, etc. When hundreds of design features exist in a facility, it is convenient to list the “generic” control in the DSA/TSR as opposed to hundreds of individual controls. (DOE-STD-3007-YR TBD, section IV) There are no requirements for DOE approval of the CCR in the draft Standard. Is it the intent that if generalized controls are employed in the DSA/TSR, the CCR should be treated as if it were the TSR (and thus specifically approved by DOE) as opposed to being a technical reference that does not require DOE approval?




12. Answer. ***No. The CCR is intended to be the contractor produced document that states - we have looked at all NCS controls using a defined set of review criteria and the following controls (if any) are the only ones that require protection beyond that provided by the NCS Program and therefore will become DSA/TSR level controls. The document itself is supposed to be a technical reference document not a DOE approval document.***



13. The beyond design basis discussion seems to imply that CSEs have a listing of contingencies that were dismissed as not credible. (DOE-STD-3007-YR TBD, section IV B) While there may be some incredibility discussions in CSEs, for the most part CSEs do not list what was not evaluated, nor does there appear to be any requirement to do so in the draft Standard. Is the intent to require such a listing?

No.



14. The CCR appears to be designed to identify those controls that flow forward as TSR level controls requiring DOE/NNSA prior approval to modify those control.

- 14.1 Is that understanding correct? **YES**

- 14.2 Does the CCR have to list all the controls in the CSEs, or only those being elevated to the TSR level treatment? ***Only those being elevated. A discussion of what was evaluated must be contained in the document but it is not necessary to specifically list each and every control. Reference to the CSE is sufficient.***