This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

2018 EFCOG Nuclear Facility Safety Conference
Richland, WA, August 11-17, 2018

SAND2018-7845C

Application of DOE Standard 3009-2014 to the Development of Documented Safety Analyses for Research Reactors

Darren G. Talley and Anthony L. Baca
*Sandia National Laboratories**
P.O. Box 5800, Albuquerque, NM, 87185-1141
dgtalle@sandia.gov, abaca2@sandia.gov

Abstract

The 10CFR830 safe harbor methodology for reactor nuclear facilities, such as the Annular Core Research Reactor (ACRR) and Critical Experiments (CX) at Sandia National Laboratories (SNL), is Regulatory Guide 1.70 (RG 1.70), which was designed for commercial nuclear reactor power plants. Since the DOE issued Subpart B of 10 CFR 830, significant experience has been gained in its application to *nonreactor* nuclear facilities using the DOE Standard 3009 (DOE-STD-3009) safe harbor methodology. The DOE-STD-3009 approach centers around a detailed, ground-up hazard analysis, and the identification of safety class and safety-significant structures, systems, and components. The hazard analysis and safety class/safety-significant categorization have become an expectation for reactor nuclear facilities, even though RG 1.70 methodology does not require a detailed hazard analysis, nor does it have safety class/safety-significant categories. This has resulted in hybrid methodologies in which reactor nuclear facilities "fit" ground-up hazard analyses and safety class/safety-significant designations into a RG 1.70 Documented Safety Analysis (DSA). Further, methodological conflicts arise when RG 1.70 requires designation of safety limits where 10 CFR 830 definitions and DOE-STD-3009 methodology criteria would not result in designation of safety limits. This work seeks to define an approach by which an extended DOE-STD-3009 methodology may be utilized to develop research reactor facility DSAs. The approach would maintain consistency with 10CFR830 definitions and the general DOE-STD-3009 methodology, while accommodating the unique operational and accident scenario characteristics of a nuclear reactor within the development of a ground-up hazard analysis.

*Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia Corporation, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

Introduction

Sandia National Laboratories (SNL) operates two reactor nuclear facilities: the Annular Core Research Reactor (ACRR), and the Sandia Pulsed Reactor Critical Experiments (CX) Facility. The ACRR is a small research reactor, primarily utilized in a pulse mode where power can reach ~30 GW, but for less than 10 ms. In its steady-state mode, the reactor's maximum power level is just under 2.5 MW. The CX is primarily used in a zero-power approach-to-criticality mode to obtain nuclear criticality benchmark data. As Department of Energy (DOE)[1] nuclear facilities, each must maintain a Documented Safety Analysis (DSA) and Technical Safety Requirements (TSR) which meet the safety regulations contained in Subpart B of 10 CFR 830 – the Nuclear Safety Management rule (Ref. 1).

While not formally prescribing any one particular DSA preparation methodology, the rule delineates (in Table 2 of Appendix A to Subpart B) a selection of "acceptable methodologies" that a contractor may use without prior DOE approval. These acceptable methodologies (commonly referred to in the DOE community as "safe harbor" methodologies) are delineated based upon the type of nuclear facility. The safe harbor methodology for these two SNL reactors (and all other DOE reactors) is the Nuclear Regulatory Commission's Regulatory Guide 1.70 (RG 1.70) - *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants* (Ref. 2). We note that aside from these two SNL reactors being significantly different from each other in power level and operational purpose, they are both *very* different from the commercial power plant reactors for which RG 1.70 was intended. Before proposing an alternate methodology for small research reactors such as ACRR and CX, we will examine the background in which 10 CFR 830 safe harbors came to be.

Background

The initial portions of 10 CFR 830 (§§830.1-830.7 and §830.120, Subpart A) were issued on April 5, 1994 (Ref. 3), and dealt primarily with quality assurance requirements for DOE nuclear facilities. At this time, the DOE Office of Environmental Management (DOE/EM) was undertaking cleanup activities which would eventually include over 100 sites across the United States. These activities ranged from processing of spent nuclear fuel and other high level radioactive waste for disposal, to storage sites for low level radioactive waste, to cleanup of residual low level soil contamination.

[1] For brevity, this paper includes National Nuclear Security Agency nuclear facilities when referring to DOE nuclear facilities.

At that time, this would have necessitated the development of a significant number of safety analysis reports under DOE Order 5480.23 for these various types of *nonreactor* nuclear facilities. A new standard, DOE-STD-3009-94 (Ref. 4), was initially issued in July 1994 specifically for the development of *nonreactor* nuclear facility DSAs. Work continued on DOE-STD-3009-94, and on the development of Subpart B to 10 CFR 830, which would address safety basis requirements DOE nuclear facilities. Change Notice 1 for DOE-STD-3009-94 (Ref. 5) was issued in Jan. 2000. Meanwhile, Subpart B of 10 CFR 830 was finalized in January 2001. Shortly thereafter, DOE-STD-3009-94 Change Notice 2 (Ref. 6) was issued in April 2002.

In Table 2 of Appendix A to Subpart B, the rule listed safe harbor methodologies for several types of nuclear facilities. Except for reactor nuclear facilities and transportation activities, DOE-STD-3009-94 Change Notice 1 (or its successor documents) is listed as either an acceptable methodology, or part of the acceptable methodology for all but two of the other nonreactor/non-transportation nuclear facility types. The other two safe harbor methodologies in Table 2 (DOE-STD-1120-98 and DOE-STD-3011-94) are arguably scaled-down versions of the DOE-STD-3009[2] methodology, for a more targeted application to the deactivation and decommissioning of a DOE nuclear facility. The DOE-STD-3009 methodology was apparently considered to be well-established and applicable to a broad range of nuclear facilities.

<u>The Influence of DOE-STD-3009 on "Non" Nonreactor Nuclear Facilities</u>

The subsequent influence of DOE-STD-3009 within DOE nuclear facility directives and standards is pervasive. One could conceivably conclude that the DOE directives and standards for nuclear facilities have been, or are being transformed, in a manner which most directly relates to DOE's nonreactor nuclear facilities and to DOE-STD-3009. Consider the example of DOE Order 420.1C, Change 1 (Ref. 7).

- The change note in the order explicitly states the changes were intended to invoke DOE-STD-3009-2014 (Ref. 8) as a required method.
- The Nuclear Safety Design Criteria chapter in Attachment 2 applies to new nuclear facilities, with no distinction made between nonreactor and reactor nuclear facilities.
- Contractors are required to identify safety class and safety-significant SSCs, concepts which within DOE are only practically developed in DOE-STD-3009 with its Evaluation Guideline.
- Contractors are required to use DOE-STD-1189-2008, *Integration of Safety into the Design Process* (Ref. 9), which relies heavily upon the DOE-STD-3009 methodology.

[2] Also for brevity, and since successor documents are also acceptable methodologies, "DOE-STD-3009" will be used as a shorthand moniker, unless reference to a specific version of the Standard is intended.

Other methodologies are not precluded, but the language and construction of DOE-STD-1189 is highly focused toward a DOE-STD-3009 safety basis.

- Chapter V of DOE O 420.1C prescribes a Cognizant System Engineer program to address active safety class and safety-significant SSCs "as defined in the facility's DOE-approved safety basis documentation." This would seem to presume that even when other safe harbor methodologies may have been used, they have been adjusted to include identification of safety class and safety-significant SSCs.
- Lastly, Attachment 3 to DOE O 420.1C sets forth design criteria for safety SSCs in new nuclear facilities, distinguishing between safety class and safety-significant SSC. This would again seem to presume any other safe harbor methodology was adjusted to distinguish these types of SSCs.

DOE Guide 421.1-2A, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830* (Ref. 10), has some interesting statements regarding DOE-STD-3009 and its apparent preeminence among the safe harbor methodologies. One finds the following on p. 6 of the Guide:

> Each of the safe harbors has a methodology specific to the application to satisfy the requirements for the development of a DSA as described in 10 CFR 830.204 for the hazards identification, safety analysis, and derivation of hazard controls. DOE-STD-3009, Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facilities Documented Safety Analysis, is a safe harbor for any of the specialized areas covered by the other safe harbors (with the exception of Hazard Category 1 nuclear reactors) and can be used in lieu of any of them. An expectation associated with any of the safe harbors is that the safety classification guidance for safety SSCs (i.e., safety class and safety significant SSCs) and specific administrative controls (SACs) of DOE-STD-3009 will be used in developing the DSA.

Just below this passage on p. 6, the Guide states the following:

> Most DOE large reactors use Regulatory Guide 1.70, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants. There is an ANSI/ANS standard that provides guidance for small research reactors (ANSI/ANS-15.21, I). NUREG-1537, Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors, also provides guidance for nonpower reactors. However, none of these reactor formats was written for DOE reactors and each has left out several topics that should be included. For DOE reactors, in addition to the topics discussed in Regulatory Guide 1.70, hazard analysis and categorization of the facility and applicable facility design codes and standards should be added. DOE-STD-3009 provides specific guidance for the content and organization DOE expects for these additional topics. DSAs for reactors often use different safety classification terminology (e.g., conforming to NRC Regulatory Guide 1.70) rather than that identified in 10 CFR 830.

In the first passage, the Guide sets an expectation that the DOE-STD-3009 methodology for classifying safety class and safety-significant SSCs, and determining specific administrative controls (SACs) would be necessary even for a reactor facility using RG 1.70 as its safe harbor. In the second passage, the Guide identifies perceived shortcomings of not only RG 1.70, but also other non-DOE safety analysis methodologies for small research reactors. It further states that hazard analysis and categorization, and applicable facility design codes and standards should be added to the RG 1.70 methodology, using DOE-STD-3009 to meet the expectations of DOE for these topics. At a minimum, this would presumably invoke the need for unmitigated hazard/accident analyses to determine SSC classification.

Interestingly, the Guide also states that DOE-STD-3009 can be used in lieu of any of the other safe harbors, for any specialized area except for Hazard Category I nuclear reactors. One could presume, then, that DOE-STD-3009 would be an acceptable methodology for a Hazard Category 2 nuclear reactor.

<u>The Use of RG 1.70 as a Safe Harbor Methodology</u>

None of the above discussion of the pervasiveness of the DOE-STD-3009 methodology is intended to discount the acceptable use of RG 1.70 as a methodology for producing a safety analysis case for a reactor. RG 1.70, however, was intended for a broad, but specific class of reactors (i.e., commercial light water power reactors), and to demonstrate compliance (primarily) with 10 CFR 50 regulations for NRC-regulated reactors. If strictly followed, the result would be a safety analysis report which meets the requirements of 10 CFR 50.34, and technical specifications which meet the requirements of 10 CFR 50.36. This would include comparison of dose consequences to 10 CFR 100.

However, it is obviously incumbent upon DOE reactor nuclear facilities to comply with 10 CFR 830 Subpart B requirements, and the RG 1.70 safe harbor methodology has limitations in this respect. For example, if one strictly follows the RG 1.70 methodology to a DOE reactor nuclear facility, the resulting DSA

- Would not perform a hazard analysis of other facility operations not directly related to the reactor and its operation (e.g., experiment preparation, handling, irradiation, and storage).
- Would not perform unmitigated dose consequence analyses and apply the DOE Evaluation Guideline to identify and distinguish safety class and safety-significant SSCs.
- Would not identify administrative functions or actions which would be safety class and/or safety-significant if performed by an SSC, (i.e., would not identify SACs).

RG 1.70 was written for high power commercial reactor power plants. With the high power level of such reactors, there is the *presumption* of a high dose consequence potential. This presumption results in presumptions regarding the safety SSCs of the reactor power plant facility. The application of RG 1.70 to a much lower power research reactor of critical assembly then has implications for the resulting DSA. If one strictly follows the RG 1.70 methodology, the resulting DSA

- Would identify safety limits for the fuel and/or reactor coolant pressure boundary irrespective of dose consequence potential.
- Would identify limiting safety system settings (vs. limiting control settings) for reactor scram systems to protect identified safety limits irrespective of dose consequence potential.
- Would identify SSCs such as containment systems, emergency core cooling systems, control room ventilation systems, and fission product filtration systems to be safety-related, with no distinction between safety class, safety-significant, or neither, and without regard to dose consequence potential.

DOE reactors currently range from low/zero-power critical assemblies, to 2.5 MW research reactors, to 85 MW and 100-250 MW test reactors. For the higher power DOE reactors, there is a relatively high dose consequence potential, and some of the implications above may not cause undue concern in applying the RG 1.70 methodology. However, when applied to a low power research reactor or critical assembly, the use of RG 1.70 in a one-size-fits-all manner can be inefficient and potentially misleading. For example, reactor cooling systems, reactivity control systems, pressure boundaries, reactor vessels, containment systems, emergency core cooling, instrumentation and controls, electric power, auxiliary systems, etc., are all addressed as safety related in RG 1.70, regardless of their importance for a research reactor or critical assembly safety and operations. Identification of safety limits for low dose consequence potential reactors invites confusion over the perceived hazard level of the facility. Not ascribing safety class or safety-significant status to certain SSCs invites criticism for not meeting the intent of the safe harbor methodology. And, perhaps most importantly, the presumption that the reactor itself is the primary hazard, fails to respect the potential that fissile material-containing reactor experiments and/or reactor fuel handling and storage activities may actually present the more significant dose consequence potential.

Again, the identification of such issues is not necessarily intended to deter the use of RG 1.70 for reactor facilities, especially for Hazard Category 1 reactor nuclear facilities. For lower hazard reactor facilities, such as the ACRR and CX, one might consider the NUREG-1537 methodology (Ref. 11). However, one would again be dealing with a methodology developed to comply with 10 CFR 50 requirements, albeit tailored for research reactors vs. commercial power reactors. The ANSI/ANS-15.21 standard (Ref. 12) for research reactor safety analysis report format and content is similar in construction to NUREG-1537, but without an emphasis on any particular regulatory environment. To use RG 1.70, or either of these potential alternatives, one must also address the additional work necessary to ensure full compliance with 10 CFR 830. While this additional-work approach is acceptable, the purpose of this paper is to propose an alternate approach.

The Proposed Use of DOE-STD-3009-2014 for Reactor Nuclear Facilities

An alternate methodology to RG 1.70 is proposed for low power research reactors and critical assemblies to address the issues noted above. The proposed alternate methodology is to utilize an enhanced DOE-STD-3009-2014 methodology for the development of the DSA. DOE-STD-3009-2014 is the underlying basis for the alternate methodology for the following reasons:

- It was explicitly developed to ensure compliance with the requirements and expectations for DSA hazard and safety analysis under 10 CFR 830 Subpart B.
- Its hazard analysis process/techniques can be applied to reactor nuclear facilities as well as to nonreactor nuclear facilities.
- Its hazard analysis process will address facility activities which are not directly related to reactor operation, such as the handling and storage of reactor fuel, and the preparation, handling, and irradiation of reactor experiments.
- It provides a defensible, concise, and logical approach to identifying safety class and safety-significant hazard controls, and documenting their safety function requirements.
- Its use allows for direct, immediate, and consistent transition to compliance with DOE Orders and Standards which address safety class and safety-significant SSCs and SACs.

The characteristics of DOE-STD-3009-2014 listed above also distinguish its flexibility to apply to a wide range of research reactor and critical assembly facilities. One could describe RG 1.70 as guiding the final stages of a safety analysis documentation process, documenting previously agreed-upon hazard controls derived from the presumed hazard analysis of a commercial nuclear power plant. DOE-STD-3009-2014 provides a methodology for the full and traceable development of hazard controls from a documented hazard analysis of essentially any nuclear facility process or processes, and then the concise and organized documentation of the safety functions for the SSCs and administrative functions which the hazard analysis has demonstrated to be key in the protection of the public and the workers.

Even with these characteristics, we propose that certain enhancements to the DOE-STD-3009-2014 methodology need to be made to address reactor nuclear facilities. The proposed enhancements to the DOE-STD-3009-2014 methodology are considered necessary because of certain unique aspects of nuclear reactor safety and operation. The enhancements are drawn from the methodologies of both RG 1.70 and NUREG-1537, as well as ANSI/ANS-1-

2000 (Ref. 13) for critical assemblies. In particular, the proposed alternate methodology would enhance DOE-STD-3009-2014 by including

- <u>Requirements to Identify Specified Acceptable Fuel Design Limits (SAFDLs)</u>: The enhanced DOE-STD-3009-2014 methodology would require that the DSA identify the threshold fuel design parameters, which if exceeded, could lead to the uncontrolled release of radioactive materials.
- <u>Requirements for a Reactor Protection System</u>: The enhanced DOE-STD-3009-2014 methodology would require a reactor protection system (i.e., a scram system) to prevent damage to the reactor fuel and cladding.
- <u>Guidance for Hazard Scenario Development of Reactor-Related Events</u>: The enhanced DOE-STD-3009-2014 methodology would include instructions to consider accident event initiators and scenarios described in reactor facility safety basis development documents such as RG 1.70 and NUREG-1537, and ANSI/ANS Standard 15.21.
- <u>Instructions for an Expanded Facility Description</u>: The enhanced DOE-STD-3009-2014 would include expanded instructions for DSA format and content. The expansion would include topic headings for descriptions of the reactor, the reactor cooling system, the reactor instrumentation and control systems, and the reactor's experiment irradiation facilities.

Figure 1 provides a diagram of the areas of DOE-STD-3009 methodology which will be enhanced. The proposed enhancements will draw upon the reactor safety community experience documented in RG 1.70, NUREG-1537, and ANSI/ANS-1-2000, to ensure that the unique hazards and hazard control aspects for a research reactor facility are identified and addressed in the facility hazard and accident analysis and hazard control selection process.

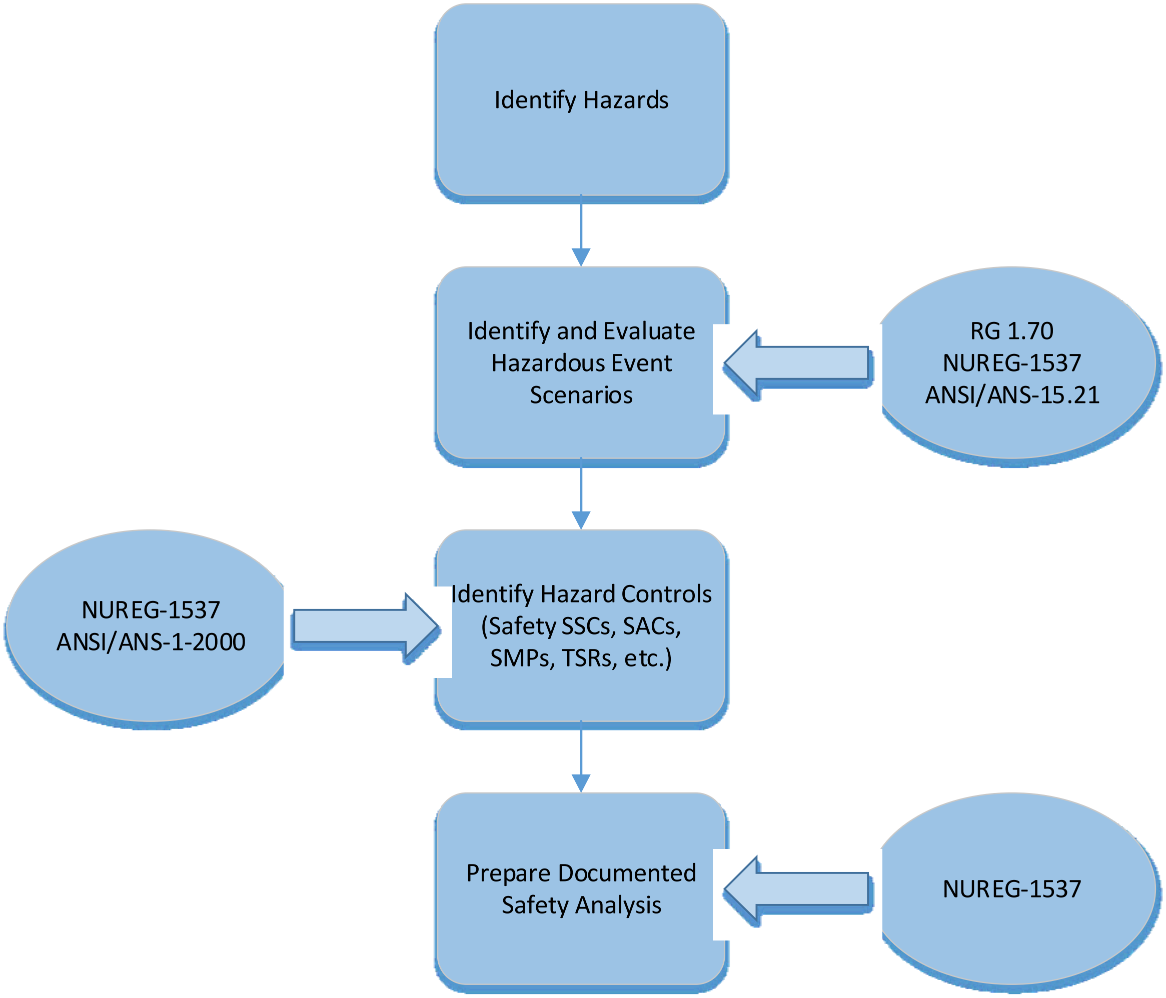

Figure 1. Depiction of the enhanced DOE-STD-3009 methodology, and the reactor safety documents which will influence the enhancements.

Requirements to Identify Specified Acceptable Fuel Design Limits (SAFDLs)

The term *SAFDLs* is borrowed from 10 CFR 50 Appendix A – *General Design Criteria for Nuclear Power Plants* (Ref. 14). These are threshold fuel design parameters which, if exceeded, could result in the uncontrolled release of radioactive material from the fuel. It is important that the DSA identify these thresholds to ensure that these are not exceeded during normal operation and anticipated operational occurrences. SAFDLs which may be identified include material melting points, yield or ultimate tensile strength, minimum allowable critical heat flux ratio, etc. The classification of the any SAFDLs as a safety limit (per 10 CFR 830 and DOE-STD-3009) will depend upon the hazard and accident analysis results as compared to the Evaluation Guideline.

Requirements for a Reactor Protection System

DOE-STD-3009-2014 is generally non-prescriptive with regard to the particular types of structures, systems, components (SSCs) employed as hazard controls. However, the primary emphasis, implicit within DOE-STD-3009, is upon confinement and filtration related SSCs, and SSCs which prevent or mitigate the spread of a fire. This emphasis is not unexpected for nonreactor nuclear facilities. In order to address reactor nuclear facilities, the DOE-STD-3009-2014 methodology will need to be enhanced to prescribe the deployment of a reactor protection system (RPS), also known as a scram system, for reactor nuclear facilities. An RPS is required by RG 1.70 for commercial power reactors, NUREG-1537 for low power research reactors, and by ANSI/ANS-1-2000 for zero power critical assemblies. The setpoints for the RPS will be selected to ensure that SAFDLs identified in the DSA are not exceeded during any normal operations or anticipated operational occurrences. The scram function of the RPS must be accomplished under the assumption that the most reactive control/safety element does not participate in the scram (i.e., under a "stuck rod" condition), and with an identified shutdown margin. The classification of the RPS (safety class, safety-significant, or not), setpoints (limiting control settings or not) and the SAFDLs (safety limit or not), will depend upon the hazard and accident analysis results as compared to the Evaluation Guideline.

Guidance for Hazard Scenario Development for Reactor-Related Events

DOE-STD-3009-2014 provides a methodology for performing an in-depth and systematic hazard analysis for a broad variety of nonreactor nuclear facilities. This same methodology is applicable to reactor nuclear facilities. A considerable experience base within the reactor operation community has identified certain anticipated operational occurrences and accident initiating events which all reactors should address. The DOE-STD-3009-2014 methodology will be enhanced with instructions to consider accident event initiators and scenarios described in RG 1.70, NUREG-1537, and ANSI/ANS 15.21. Not all of these event scenarios may be applicable to a particular research reactor facility, but it is important that the hazard analysis team's evaluations benefit from the collective hazard/accident evaluation experience of the reactor community. This approach was successfully utilized in the recent development of an updated hazard analysis for the CX DSA. Figure 2 presents a depiction of the review of NUREG-1537 accident-initiating events and their consideration for defining hazard event scenarios to be addressed in the hazard analysis.

NUREG-1537 Section 13.1 **Accident-Initiating Events and Scenarios**	**Implementation in DOE-STD-3009** **Hazard Scenario Definition**
Insertion of Excess Reactivity • Rapid inadvertent insertion of a portion of all excess reactivity loaded into the reactor. • Rapid removal of the most reactive control rod or shim rod. • Rapid insertion of a fuel element into a vacancy in the core at the most reactive position. • Ramp insertion of reactivity by drive motion of the most reactive control rod or shim rod, or ganged rods, if possible (this event could occur during reactor startup procedures or when the reactor is at power).	Define Hazard Event UER-2-2 as a rapid excess reactivity addition that bounds these scenarios.
Insertion of Excess Reactivity • Failure or other malfunction of an experiment that inserts excess reactivity (this can be used to justify movable experiment reactivity limits).	Define Hazard Event UER-2-4 related to potentially movable experiments.
Insertion of Excess Reactivity • Rapid increase in reactivity as a result of a change in operating parameters, such as a surge of cold coolant	Not Applicable. Water which may be introduced to the assembly tank is within a self-contained storage tank/recirculation system with no means of cooling the coolant.
Loss of Coolant • Failure or malfunction of some component in the primary coolant loop • Failure or malfunction of an experimental facility, such as a beam tube • Failure or leak of the reactor coolant boundary	Not applicable. Zero-power critical assembly with no appreciable decay heat, requiring no normal or emergency cooling system.
Loss of Normal Electric Power • Onsite or offsite power interruption.	Define Hazard Event EE-2-1 to address loss of electric power.

Figure 2. Depiction of the use of NUREG-1537 accident-initiators to define hazard event scenarios in the enhanced DOE-STD-3009 methodology (examples from CX DSA).

Instructions for an Expanded Facility Description

DOE-STD-3009-2014 provides instructions for the content of DSA chapters, of which Chapter 2 is to contain a facility description. The instructions further provide for addressing various facility aspects by specifying description subsections 2.1 through 2.9. To accommodate the pertinent information related to a reactor facility, the section 2.5 "Process Description" could include summary discussions of reactor operations, as well as activities related to preparing, installing, irradiating, and processing reactor irradiation experiment packages, neutron radiography, etc. At this point, however, the instructions for Chapter 2 would need to be expanded to include sections to describe the reactor itself, along with important reactor support systems. Figure 3 depicts the addition of these descriptive sections.

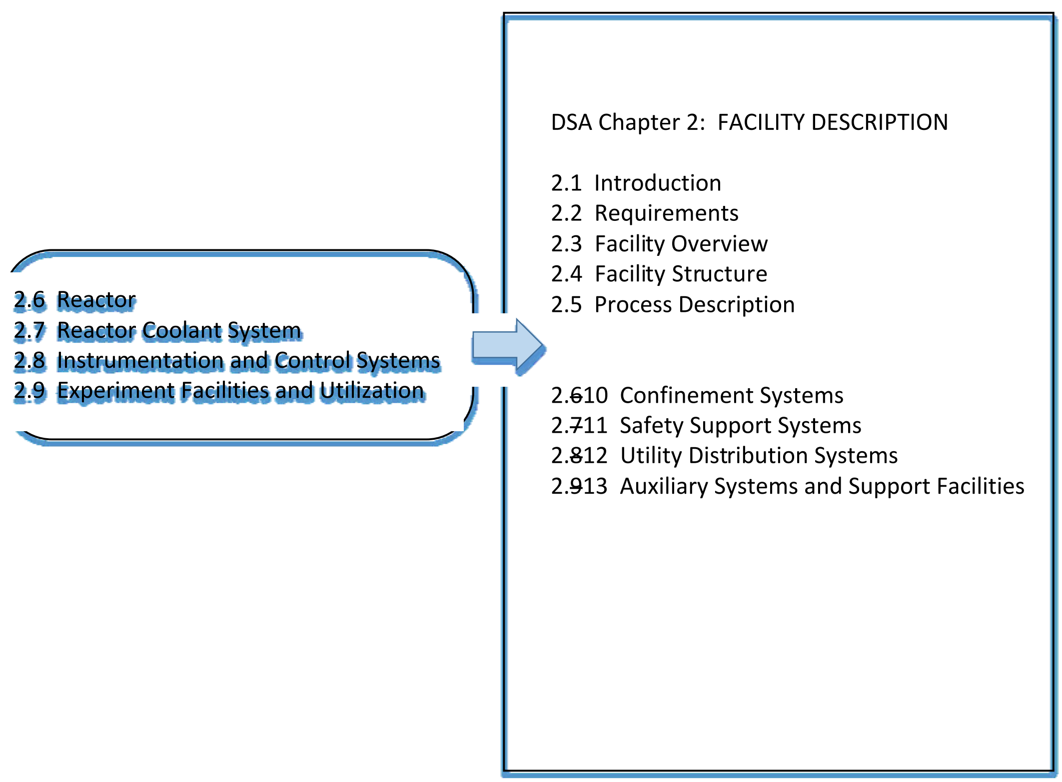

Figure 3. Diagram showing the enhancement to DOE-STD-3009's Facility Description DSA chapter.

It is proposed that NUREG-1537 be used as a guide to develop the content of the new description subsections shown in Fig. 3. This would ensure that the experience gained by the NRC research reactor community in developing appropriately detailed safety analysis descriptions of the reactor systems would be leveraged in the development of the DOE-STD-

3009 DSA. The following briefly describes the information in the subsections which would be inserted in the DOE-STD-3009 DSA in Chapter 2:

2.6 Reactor: This section would describe the reactor and its structures and components, including its reactivity control rods. The normal operating characteristics (nuclear and thermal-hydraulic) of the reactor design are described. This section would also identify and describe the SAFDLs for the fuel. The subheadings from Chapter 4 of NUREG-1537 would be recommended to organize the description, just as the content descriptions of NUREG-1537 would be used to guide the DSA preparer in selecting reactor design/operation topics to address.

2.7 Reactor Coolant System: This section would provide an overview the reactor coolant system – primary, secondary, and related subsystems. If an emergency core cooling system (ECCS) is required, an overview would be presented here, although if the ECCS were to be safety class or safety-significant, the more detailed description would be included in Chapter 4 of the DSA. The subheadings from Chapter 5 of NUREG-1537 would be recommended to organize the description, just as the content descriptions of NUREG-1537 would be used to guide the DSA preparer in selecting reactor coolant design/operation topics to address.

2.8 Instrumentation and Control Systems: This section would provide an overview the reactor instrumentation and controls systems. The would include the required reactor protection system. The subheadings from Chapter 7 of NUREG-1537 would be recommended to organize the description, just as the content descriptions of NUREG-1537 would be used to guide the DSA preparer in selecting reactor instrumentation and control and protection system design/operation topics to address.

2.9 Experiment Facilities and Utilization: This section would provide an overview the features and SSCs of the reactor which facilitate the irradiation of "experiments." Examples could include irradiation tubes or cavities, neutron beam ports, neutron radiography ports, etc. This section would also describe the manner in which these experiment facilities are used. The subheadings from Chapter 10 of NUREG-1537 would be recommended to organize the description, just as the content descriptions of NUREG-1537 would be used to guide the DSA preparer in selecting experiment facility topics to address.

Conclusion

The safe harbor methodology for DOE reactor facilities may be appropriate for higher power (85-100 MW) reactors, but it less appropriate for lower power (e.g., 2.5 MW) and zero-power critical assemblies. The search for an alternate methodology for these lower power reactor facilities should consider the pervasive impact of DOE-STD-3009 within the DOE safety analysis community. While potential alternate methodologies such as NUREG-1537 and ANSI/ANS-15.21 may be attractive, they do not offer a straightforward means of demonstrating compliance with 10 CFR 830 Subpart B as is offered by DOE-STD-3009. This work has proposed that an enhanced DOE-STD-3009 may be used to address the development of a reactor facility safety basis. The enhancements, being drawn from RG 1.70, NUREG-1537, ANSI/ANS-15.21, and ANSI/ANS-1-2000, are thus rooted within the broad experience base of the reactor operation community, and are easily merged with the DOE-STD-3009 methodology.

The use of the well-established methodology of DOE-STD-3009-2014 will ensure compliance with 10 CFR 830 Subpart B, providing for the performance of a complete facility hazard and accident analysis, identification of safety class and/or safety-significant hazard controls, and the derivation of facility Technical Safety Requirements. The use of the DSA format and content expectations within DOE-STD-3009-2014 will ensure a systematic documentation and communication of the safety basis in a format familiar to internal and external DOE oversight agents and directly consistent with nuclear facility related DOE Orders and Standards.

References

1. *Subpart B—Safety Basis Requirements*, 10 CFR 830, Nuclear Safety Management.
2. NRC Regulatory Guide 1.70, *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants (LWR Edition)*, Revision 3, November 1978.
3. *10 CFR 830 Nuclear Safety Management*, Federal Register, Vol. 59, No. 65, April 5, 1994, p. 15843.
4. DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, July 1994.
5. DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, Change Notice 1, January 2000.
6. DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis*, Change Notice 2, April 2002.
7. DOE O 420.1C, *Facility Safety*, Change 1, February 27, 2015.
8. DOE-STD-3009-2014, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analysis*, November 2014.
9. DOE G 421.1-2A, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830*, December 19, 2011.
10. DOE-STD-1189-2016, *Integration of Safety Into the Design Process*, December 2016.
11. NUREG-1537, *Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors*, dated February 1996.
12. ANSI/ANS-15.21-1996, *Format and Content for Safety Analysis Reports for Research Reactors*, November 29, 1996.
13. ANSI/ANS-1-2000, *American National Standard for Conduct of Critical Experiments*, March 23, 2000.
14. *Appendix A to Part 50—General Design Criteria for Nuclear Power Plants*, 10 CFR 50, Domestic Licensing of Production and Utilization Facilities.