Maximum Credible Accident Methodology

Summary of Methodology

October 2020

Oklo Inc., Non-proprietary

TABLE OF CONTENTS

TABLE OF FIGURES

1 PURPOSE AND SCOPE

The purpose of this report is to summarize the methodology and approach to transient and accident analyses performed by Oklo Inc. (Oklo) for the licensing bases of its reactors. These analyses cover a spectrum of events within the design bases of the unit as well as consideration of beyond design basis events and severe events. The results of transient and accident analyses demonstrate:

- An adequate unit response to challenging conditions,
- Conformance with applicable regulations concerning structures, systems, and component (SSC) performance and postulated radiological consequences, and
- The expectation of adequate protection of the public during the unit lifecycle.

Oklo employs a maximum credible accident (MCA) methodology to guide this analysis. The MCA methodology systematically provides an understanding of which functions have an effect on plant safety, and therefore which functions or inherent features should be regulatorily controlled. This leads to the creation of regulatory criteria for those functions and inherent features within the NRC application, and the appropriate quality assurance treatment is then applied based on those criteria.

This summary document explains how this methodology is applied, and the quality assurance considerations that result from the application of the methodology. Section 2 provides an overview of the methodology. Sections 3 through 8 describe each of the major steps in the methodology, which is then summarized in Section 9. Section 10 then describes the quality assurance considerations that result from the methodology. Appendix B provides an example application of this methodology, as it is applied to the Aurora reactor.

2 ANALYSIS APPROACH

Oklo uses an MCA methodology to identify the events of highest importance in the safety analysis. The MCA methodology considers the range of potential challenges posed by possible events, groups these events together into event categories based on similar phenomenology of challenge, identifies which events in a category are bounding, and focuses analysis on these bounding events to ultimately designate a single MCA. More formally, the methodology applies the following steps to achieve both a wide-ranging yet ultimately focused analysis of the safety of the reactor:

1. Perform a literature review to understand the historical context and past challenges considered for fission reactor systems, both those that have operated and those proposed. In the context of these past events considered, determine which events are applicable for the reactor design, and what, if any, new events specific to the reactor design would be applicable.

2. Screen all applicable events to determine which ones are credible for the reactor design.

3. Group the credible events together into event categories based on similar phenomenology of challenge to safety.

4. Identify and analyze the bounding events in each category that challenge safety. Review this set of bounding events to determine whether the bounding event in one category is also bounded by the bounding event in another category, to develop a final set of overarching bounding events.

5. Identify the most challenging event to the safety of the plant based on the worst single failure or worst single cause of common cause failures, which is then designated the MCA.

6. Apply a defense-in-depth consideration by assuming a single additional failure in the system used to shut down the reactor in addition the MCA. Perform the safety analysis assuming the occurrence of the MCA with the addition of the single failure and demonstrate that the Dose Acceptance Criterion is satisfied.

In essence, the event evaluation process funnels a large number of events and progressively screens, bounds, and analyzes events until reaching a single bounding event, which is designated as the MCA. Figure 2-1 presents a visual representation of this funnel. The six steps outlined above are described in more detail in Sections 3 through 8 and summarized in Section 9. The MCA, combined with the additional single failure for defense-in-depth, is ultimately the focus of the safety analysis. Section 10 describes how quality assurance considerations are applied to the design given the results of the safety analysis.

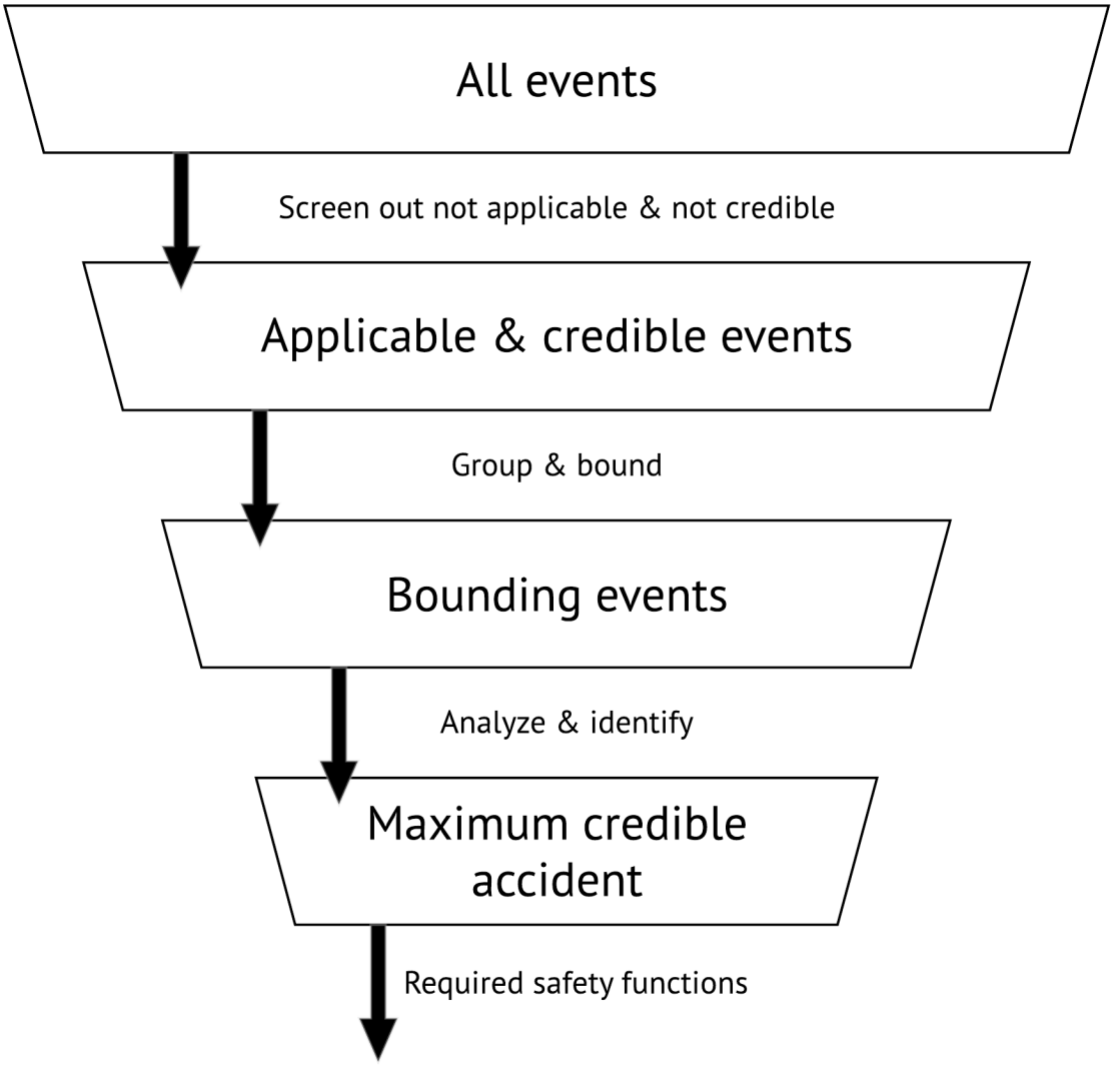

Figure 2-1: Visual representation of the event evaluation process

3 IDENTIFYING ALL POSSIBLE EVENTS

3.1 Historic identification

The methodology begins with an evaluation of previous reactor design events, both operational and conceptual. This evaluation includes the review of an exhaustive list of events, including all of the following types of resources:

- Generic events to all nuclear reactors
- Light water reactor events
- Reactor events, operating experience, and analytical methods for advanced reactors of similar design (fuel type, size, etc.)
- Expert opinion on similar conceptual designs

It is not intended that all resources will have the same relevance and this consideration must be taken into an account during this process. Reactor designs with similar design features should be considered with heavier importance than those that do not have similar designs. Additionally, events that are deemed reasonable for the design can be added to this list. Although Oklo does not anticipate developing light water reactor designs, light water reactors have important operational experience and are a good candidate for event consideration.

3.2 Determination of applicability

After all potential events are identified, a systematic down selection for relevance must occur in order to identify applicability to the design. This down selection should involve a mechanistic consideration of the event against the given design as well as an explanation of the possibility of the event occurring. Specifically, this down selection considers whether the event is applicable in terms of phenomenology. This determination is made according to "Criterion 1," which is summarized in the box below.

Criterion 1: Screening events for applicability

An event is applicable if the phenomenology of the event is relevant to the design. Events that are deemed applicable to the design under evaluation pass Criterion 1 and proceed for further evaluation.

Events that do not pass Criterion 1, meaning they are not applicable to the design, are screened out of the safety analysis and are not further analyzed. Events that do pass Criterion 1 continue through the safety analysis pipeline. The following are example applications of Criterion 1:

- A heat pipe failure event would not be considered for a reactor that does not utilize heat pipes. This event would fail Criterion 1 and not be analyzed further.

- A failure of a backup sodium tank would not be considered for a reactor that does not utilize sodium coolant. This event would fail Criterion 1 and would not be analyzed further.

- A spurious rotation of control drums would be considered for a reactor that uses control drums for reactivity control. This event would pass Criterion 1 and would be analyzed further.

4 EVALUATING CREDIBILITY OF EVENTS

After Criterion 1 has been applied to the large list of potential events, the events that passed through Criterion 1 are further analyzed for credibility. The determination of credibility is made according to "Criterion 2," which is summarized in the box below.

Criterion 2: Screening events for credibility

The credibility of events is determined via a two-step process, and events must pass both sub-criteria to pass Criterion 2:

A. The event is physically, fundamentally, or mechanistically possible.

B. The event could be caused by a single initiating event, that could result in a common set of failures, even if extreme.

Events that are credible for the reactor design under evaluation pass Criterion 2 and proceed for further evaluation.

Criterion 2A is a screening tool for events that might not be physically, fundamentally, or mechanistically possible. It is different than Criterion 1 because the physical features analyzed do exist, and therefore the associated events have already been deemed applicable. Criterion 2A analyzes whether those events could actually occur in the reactor design under evaluation. Continuing with the example from the previous section that passed Criterion 1, the application of Criterion 2A to the spurious drum rotation would proceed as follows:

- A spurious drum rotation postulating drum rotation speeds that are not possible given the mechanical design of the control drum system would fail Criterion 2A and would not be analyzed further.

- A spurious drum rotation postulating drum rotation speeds that are possible given the mechanical design of the control drum system would pass Criterion 2A and would be analyzed further.

Criterion 2B is a screening tool for events to ensure that they are caused by a single initiator. This single initiator could cause subsequent failures, including a common set of failures, however, these subsequent failures must be within the bounds of criterion 2A (i.e., be physically, fundamentally, or mechanistically possible). The entire event sequence must be mechanistically possible. In the example of spurious rotation of control drums, the postulated drum rotation would only pass Criterion 2B if it could be caused by a single initiating event that results in the postulated rotation. If the postulated drum rotation required multiple, separate initiating events, it would be screened out by Criterion 2B and deemed not credible.

The application of Criterion 2 is a systematic review of the events that have passed through Criterion 1. Ultimately, the identification of an event as "credible" means that it has passed both Criterion 1 and Criterion 2. Credible events then proceed to be evaluated further.

5 GROUPING OF EVENTS

After the initial list of all potential events has been analyzed for applicability under Criterion 1, it is possible a large number of events remain. It is appropriate to group these events into "event groups" to reduce the analytical burden. This grouping could occur either before or after the events pass through Criterion 2. The decision for when to group events is left to the judgement of the analyst.

Grouping of events is common practice in safety analysis for reactor designs and can largely reduce the analytical burden. To continue the previous example, if control drums are used to control the reactivity of the plant, their different malfunctions could be grouped as "reactivity insertion events" and "reactivity withdrawal events."

6 PERFORMING BOUNDING ANALYSES

After the events have passed through Criterion 2 and have been grouped, the analysis of the system response is conducted. Typically, the first step of the analysis is to identify the bounding event from each event group. This step of identifying a bounding event is optional but allows for the analysis of a single event, rather than many events, in each event group. The purpose of this allowance is to reduce the overall analytical burden since an analysis of a conservatively large bounding event could encompass analyses of smaller related events. If this bounding approach is used, its appropriateness must be clearly justified and documented.

For example, a partial loss of electrical power could be bounded by a larger analysis that evaluates a full loss of electrical power. This larger, bounding analysis would be appropriate and should be documented as such. Conducting this bounding analysis would reduce the analytical burden of having to run multiple event analyses for different degrees of loss of electrical power.

Most events, or bounded event groups, are expected to not result in a dose consequence above the normal operation of the plant. For these zero consequence events, this step of the methodology allows for the termination of their analysis. Note that it is still possible that such events could be considered as the MCA in the case that all identified events have zero consequence.

The only acceptance criteria for the safety analyses described in this methodology is that of offsite dose consequence. Specifically, this criterion is related to the regulatory limit for siting, as per Title 10 of the *Code of Federal Regulations* (10 CFR) Part 100, "Reactor Site Criteria." It is referred to here as the "Dose Acceptance Criterion," and is summarized in the box below. If the safety analysis for an event does not meet the Dose Acceptance Criterion, the methodology is terminated at this step and the design of the reactor must be changed to ensure that the no events exceed this criterion. If the safety analysis passes the Dose Acceptance Criteria for all events the analysis can proceed to selecting the MCA.

Dose Acceptance Criterion

The Dose Acceptance Criterion is based on the regulatory limit for siting, as per 10 CFR Part 100. The safety analysis must meet both sub-criteria below to pass this acceptance criterion.

A. An individual located at any point on the boundary of the exclusion area for any 2 hour period following the onset of the postulated fission product release, would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).

B. An individual located at any point on the outer boundary of the low population zone, who is exposed to the radioactive cloud resulting from the postulated fission product release (during the entire period of its passage) would not receive a radiation dose in excess of 25 rem total effective dose equivalent (TEDE).

7 SELECTING THE MCA

The last step in this methodology is to select the MCA, which is the most challenging event to the safety of the plant based on the worst single failure or worst single cause of common cause failures. After every event, or bounded event group, has been identified and analyzed, it is possible to propose different events to be the MCA. The ultimate decision on which event will be the MCA will vary design-by-design. It may consider potential consequences, calculated dose, or even risk insights. Regardless, this step of the process should be thoroughly documented.

Note that external hazards are not considered as part of the down-selection process described in this MCA methodology summary, which is for internal events only. Nevertheless, external hazards are an important consideration in the safety analysis process. Therefore, after the MCA is selected, external hazards are analyzed against the design to assure that the MCA is upheld. The detailed methodology for the analysis of external hazards is outside the scope of this summary.

8 APPLYING THE DEFENSE-IN-DEPTH CONSIDERATION

After the MCA has been identified, a defense-in-depth consideration is applied. Specifically, this defense-in-depth consideration involves the application of a single failure in conjunction with the event sequence.

The consideration of single failure is not a regulatory requirement and is therefore only applied to satisfy the regulatory philosophy of defense-in-depth. The following regulatory documents were considered in the drafting of this consideration:

- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants"
- SECY 77-0439, "Single Failure Criterion"
- RG 1.53, "Application of Single-Failure Criterion to Safety Systems"
- SECY 03-0047, "Policy Issues Related to Licensing Non-Light-Water Reactor Designs"
- SECY 05-0138 "Risk-Informed and Performance-Based Alternatives to the Single-Failure Criterion"
- NRC technical report, "Technical Work to Support Evaluation of a Broader Change to the Single-Failure Criterion"
- 10 CFR Part 50, Appendix K, "ECCS Evaluation Models"

This methodology is conservative in its application because the NRC has historically taken "single failure" to only be applied to safety-related components and their safety-related functions, whereas this methodology applies single failure to the most limiting component for the event, regardless of safety classification.

This methodology does not dictate what the single failure must be, however, the single failure selected must be the most limiting failure at the time of the event. This single failure is generally taken to be a failure within the system used to shut down the reactor in response to the MCA. Risk insights from probabilistic risk assessment are used to identify the most limiting single failure within that system with a reasonable failure frequency. (Generally greater than 1×10^{-6} per reactor year, as observed for beyond design basis event analysis. Greater than 1×10^{-7} may be utilized for extra conservatism).

After identifying the most limiting single failure, the MCA is analyzed with the addition of that failure. The event is again compared against the Dose Acceptance Criterion to ensure that the criterion is still met after introduction of the additional failure. If the criterion is not met, the design of the reactor must be changed. If the criterion is met, the safety analysis is complete, and the final MCA has been identified and shown to be acceptable.

9 SUMMARY OF METHODOLOGY AND MCA SELECTION

The methodology provided in this document is one way of selecting an abnormal event that is bounding for the facility. This approach is intended to be used with smaller facilities, not because it is not possible to apply it to larger facilities, but because that application might be too restrictive. The safety analysis under this methodology starts with a thorough review of all possible events, screens those events for applicability and credibility, allows for the grouping of events, performs bounding analyses, and finally selects an MCA. The safety analysis methodology is summarized in Figure 9-1. This down-selection methodology does not consider external events, but after the MCA is selected external hazards are analyzed against the design to assure that the MCA is upheld.

After the identification of the MCA, a defense-in-depth consideration is applied. This consideration assumes an additional single failure, chosen to be the most limiting single failure at the time of the event. The safety analysis is then conducted assuming the occurrence of the MCA and the additional single failure, and the result is compared against the Dose Acceptance Criterion. If the criterion is satisfied, the final MCA has been identified and shown to be acceptable.

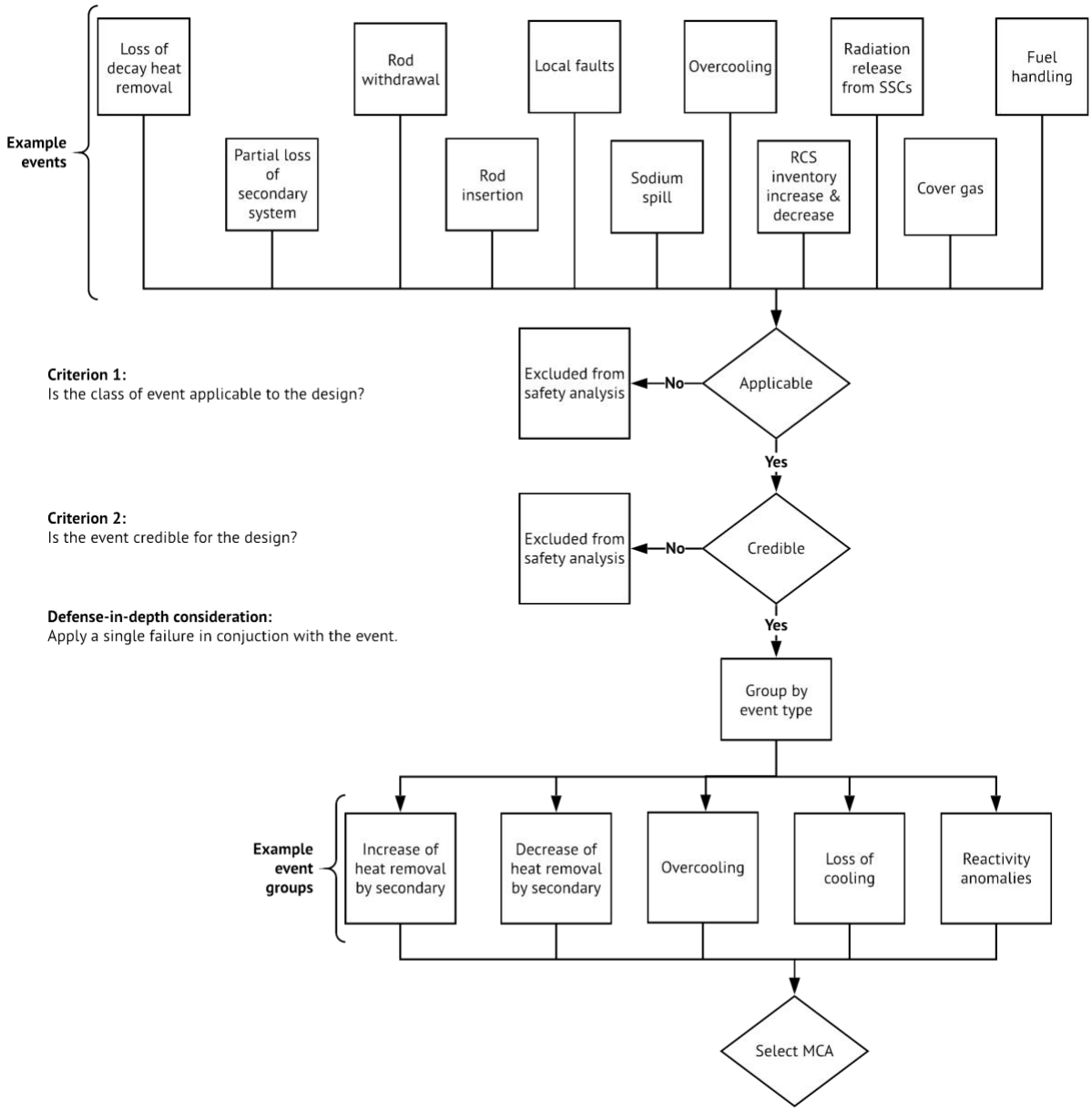

Figure 9-1: Summary of safety analysis methodology

10 QUALITY ASSURANCE CONSIDERATIONS

10.1 Methodology

10.1.1 Component classification background

"Component classification" is a widely applied term in the nuclear regulatory space but is generally interpreted as the effect of the component's functionality to the safety of the plant. Often, the term "safety classification" is used in place of "component classification," and generally there is confusion in the meaning of the terms. Further, "safety classification" is not used, not defined, and not required by 10 CFR and is therefore not a regulatory requirement for the filing of an NRC license application. Oklo conducted an exhaustive review of how terms relating to safety have been used, both historically and in recent industry regulatory interaction, which informed this methodology and is included in Appendix A: Regulatory review of safety terms.

The ultimate purpose of what is commonly referred to as "component classification" or "safety classification" is to provide a framework in which different levels of quality requirements can be applied to components, systems, or processes. In the scope of the regulator, the focus is on fulfilling those functions that are required for the safe operation of the facility. Safe operation of the facility is one during which radiation levels are not above the regulatory limits of 10 CFR, neither to the people nor to the environment, and during which the common defense and security of the nation is not compromised or significantly threatened. In addition to the scope of the regulator, there is the much broader operational scope of quality assurance, which concerns the reliable operation of the facility. Generally, the operational scope of quality assurance is much broader and much more stringent than the scope of the regulator and, ultimately, a facility that operates well will be inherently safe.

A complex framework of quality assurance is not needed in order to ensure the safe operation of a facility. For example, large light water reactors have operated safely for over 50 years in the U.S. under a simple framework. Further, advanced reactors are generally much smaller and utilize many more passive components and inherent features than the currently operating large light water reactor fleet. As such, a complex framework for assuring safety would be a step backwards, both for the industry and for the nuclear regulator. It is possible to provide assurance of adequate protection in the nuclear context with a simple approach to quality assurance.

10.1.2 Applicability of "safety-related" definition in 10 CFR 50.2

The definition of "safety-related" in 10 CFR 50.2, "Definitions," is replicated below:

> *Safety-related structures*, systems and components means those structures, systems and components that are relied upon to remain functional during and following design basis events to assure:
>
> (1) The integrity of the reactor coolant pressure boundary
>
> (2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or

> (3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable.

Of specific note is that this definition uses "safety-related" in the context of SSCs. This 10 CFR 50.2 definition is not applied to Oklo designs because it is in the context of a component-based analysis and in the context of the currently operating fleet of large light water reactors.

The NRC included this definition in its regulations after the first large light water reactors had already been operating for a number of years.[1] The concept of "safety-related structures, systems, and components" was first incorporated into the Commission's regulations in 10 CFR Part 100, Appendix A, "Seismic and Geologic Siting Criteria for Nuclear Power Plants," in November 1973. The first regulation in 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," to include a definition of "safety-related structures, systems, and components" was 10 CFR 50.49, "Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants," in January 1983. When the NRC amended its regulations to update the criteria used in decisions regarding power reactor siting, including geologic, seismic, and earthquake engineering considerations for future nuclear power plants in December 1996 it added the definition of safety-related SSCs to 10 CFR 50.2. The NRC likely based the definition of "safety-related" on the technology that had been operating in the U.S., large light water reactors.

Although Oklo's reactor designs might have systems that are similar in nature to the systems described by 10 CFR 50.2, the intent of the safety-related definition of 10 CFR 50.2 is to be taken as a whole, not piecemeal. In other words, the combination of systems described in 10 CFR 50.2 are needed to meet the safety-related definition, not any piece on its own merit, to achieve the philosophy of defense-in-depth for light water reactors. As such, a piecemeal application of a regulatory definition is not only unprecedented but is also technically inadequate for nonlight water reactors. Further, the methodology presented here describes "safety-related" in the context of functions and inherent features, not in the context of a component-based approach; this is a significant difference in interpretation of the language and another reason why the 10 CFR 50.2 definition is not applied to the Oklo designs. Lastly, definitions included in 10 CFR are not regulatory requirements and were not included by the NRC with the intention of evoking further regulatory requirements.

10.1.3 Oklo approach to component classification

Oklo has proposed a simpler approach to component classification than has been discussed in recent years. Specifically, functions and inherent features are either considered to be safety-related or not.[2] Safety-related is used only for functions or inherent features that are needed to keep dose consequences to levels below those allowed by 10 CFR for accident scenarios in the context of siting requirements. Specifically, these are the regulatory limits contained in 10 CFR Part 100 and are needed for siting purposes, as the only purpose of these dose limits is to not affect the surrounding environment. Since these limits are hard limits (i.e., not based on

[1] See "Definition of Safety-Related Structures, Systems, and Components; Technical Amendment," 62 Fed. Reg. 47268 (Sept. 8, 1997).

[2] This approach does not use other terminology, such as: safety significant, risk significant, etc.

frequency-consequence correlations) included in the regulations, this approach is largely deterministic. Those functions and inherent features that are determined to be safety-related must follow the quality assurance requirements of 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants." Safety-related inherent features are typically accounted for by identifying the characteristic of a component that provides that inherent feature, and assuring that characteristic under 10 CFR Part 50, Appendix B.

During the application of the MCA methodology, there may be a separate set of functions or a set of inherent feature assumptions that have an effect on plant safety but are not considered safety-related. This set of functions or inherent features is the result of iterative analyses between normal and abnormal operation of the facility. This set of functions and inherent feature assumptions are captured by creating regulatory criteria for systems or components within the NRC application, which are referred to as "design bases" and discussed in Section 10.2.

In addition to design bases, the NRC application may include a description of performance bases in order to provide overall information on the facility for the purpose of facilitating the regulatory review. These other requirements are called "performance bases" and are not relied on for safety, and as such, they do not require design commitments and programmatic controls. As a result, analyses related to the performance bases are generally not included in the NRC application. Systems that have no functions or inherent features that are relied on for safe operation of the reactor only have performance bases, and the level of detail in the NRC application is limited in scope to providing information for overall understanding of the operation of the facility.

Further, since the majority of functions and inherent features do not affect plant safety, only a small subset of component dimensions are important during the regulatory process. Since certain dimensions of components could have an effect on plant safety, regulatory criteria are committed to within the NRC application, specifically described as "key dimensions" and described in Section 10.3.

10.2 Design bases, design commitments, and programmatic controls

Design bases are the characteristics of a system that ensure the safe operation of the reactor. Most major systems in the reactor have at least one design basis, but some systems that are not relied on for safe operation do not have any design bases. Each design basis has one or more design commitments, which are the specific commitments made to ensure that the design basis is met. Each design commitment has one or more programmatic controls that are used to verify that the commitment is met.

Programmatic controls are used to verify that design commitments are met, and therefore that design bases are satisfied. These controls include preoperational tests (POTs), inspections, tests, and analysis acceptance criteria (ITAAC), startup tests (SUTs), and technical specifications (TS).

The assumptions and inputs modeled in the safety analysis are chosen to ensure that the transient analysis model reflects the characteristics described in the design bases and resultant design commitments. The programmatic controls function not only to verify that the design

commitments are met (i.e., that the as-built system is as described), but to provide assurance that the assumptions in the safety analysis are valid (i.e., that the modeled system is representative of the as-built system).

Some additional information about each system is provided for the purpose of improving overall understanding of the system. In particular, performance bases are provided for each system as a means of describing functions or inherent features of the system that are not relied on for safe operation of the reactor.

"Design basis summaries" are found throughout the NRC application and are depicted by a gray box. These design basis summaries are included for ease of regulator review and described below.

Gray summary boxes are used throughout this chapter to summarize each design basis at the end of the section describing the applicable system. These boxes contain the design basis, a summary of the evaluation that explains how the design basis is met, and a listing of the design commitments and programmatic controls that ensure the design basis is met.

The following abbreviations are used in the summaries:

- Design basis (DB)
- Design commitment (DC)
- Preoperational test (POT) (described further in the Initial Test Program)
- Startup test (SUT) (described further in the Initial Test Program)
- Inspections, tests, and analysis acceptance criteria (ITAAC) (described further in the Proposed License Conditions)
- Technical specification (TS) (described further in the Technical Specifications)

For example: a design basis (DB) for an example reactor system (AAA), the resulting design commitment (DC), and the required programmatic controls, would be listed as follows in the summary box:

DB.AAA.01 The AAA system performs sufficiently.

DC.AAA.01.A The specific characteristic of the AAA system is as follows.

SUT.AAA.01.A1 and A2 (described further in the Initial Test Program)

10.3 Key dimensions

For the purpose of understanding the function and layout of systems, key dimensions are provided that typically include schematics drawn to scale and nominal dimensions in tabular form. It is anticipated the Oklo designs will have very few key dimensions, in contrast to large

reactors, especially the large light water reactor fleet currently operating in the U.S. This reduction of key dimensions is the result of intentional design decisions and is important to this overall methodology and approach to reactor licensing. The dimensions that are fundamental in the description and analysis of SSCs and their design bases are referred to as "key dimensions."

10.4 Relationship to the QAPD

10.4.1 Structure of the QAPD

The two sections relevant to this methodology of the Oklo, Inc. Quality Assurance Program Description (QAPD): Design and Construction OKLO-2019-14-NP, Rev.1," (referred to as the QAPD) are the following:

1. Part II – "Quality Assurance Program Description Details" (referred to as Part II of the QAPD)

2. Part III – "Nonsafety-Related SSC Quality Control" (referred to as Part III of the QAPD)

The relationship of Part II and III of the QAPD to this methodology are described in the below sections.

10.4.2 Relationship of the design bases to the QAPD

The design bases are the characteristics of a system that ensure the safe operation of the reactor. As such, they have a higher level of quality assurance required by this methodology than those systems that have no implications on the safety of the plant. Therefore, the functions and inherent features described by the design basis summaries (i.e., gray boxes) in the NRC application fall under Part III of the QAPD.

A subset of the functions or inherent features ensured by design bases may be determined through the safety analysis to be safety-related. In that case the design basis summaries will explicitly indicate they must meet Part II of the QAPD rather than Part III.

10.4.3 Relationship of the performance bases to the QAPD

The performance bases are not relied on for the safe operation of the facility and are therefore separate from design bases. As such, functions and inherent features that are part of the performance bases are not discussed in detail in the NRC application and are not scoped under the QAPD.

10.4.4 Relationship of the key dimensions to the QAPD

The key dimensions are those dimensions that are fundamental in the description and analysis of systems and their design bases. As such, they are inherently part of the design bases and are treated the same as the design bases described in Section 10.4.2.

11 CONCLUSION

Oklo's safety analysis methodology is based on NRC regulation and guidance, adapted where necessary for each reactor design. The results of the safety analysis methodology demonstrate the capability for safe operation through a range of bounding design basis events and a significant degree of mitigation for any event beyond the design basis. Like their predecessor reactor designs, Oklo's designs ensure rapid and strong inherent reactivity feedback and accommodation of decay heat and system heat removal.

The results of the safety analyses are dependent on assumed system characteristics, setpoints, response times, and other component performance. Design bases, design commitments, and programmatic controls are used to confirm these characteristics, which are incorporated as assumptions in the safety analyses. Further, the use of Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC), tests as part of the Initial Test Program (ITP), and Technical Specifications (TS), during normal operation, will be used to validate and protect the assumptions made. The safety analyses may be reevaluated when changes are made in accordance with applicable regulations. Ultimately, these design bases are scoped under the QAPD to a higher level of quality assurance to ensure the safe operation of the facility.

12 REFERENCES

[1] G. T. Mazuzan and J. S. Walker, *Controlling the Atom: The Beginnings of Nuclear Regulation 1946-1962 (NUREG-1610)*. University of California Press, 1984.

[2] R. McNally, "Special Treatment for Important to Safety Structures, Systems And Components (SSCs) In The Licensing Of Light Water Reactors," presented at the ICAPP, Anaheim, CA, Jun. 2008.

[3] "Generic Letter 84-01, NRC Use of the Terms, 'Important to Safety' and 'Safety Related,'" U.S. Nuclear Regulatory Commission, Generic Letter GL 84-01, Jan. 1984.

[4] "Regulatory Guide 1.201 (For Trial Use) Guidelines For Categorizing Structures, Systems, And Components In Nuclear Power Plants According To Their Safety Significance, Revision 1." U.S. Nuclear Regulatory Commission, May 2006.

APPENDIX A: REGULATORY REVIEW OF SAFETY TERMS

A.1 Background on safety classification

Although the term "safety classification" is not defined, not used, and not required by the regulations within 10 CFR, there are many terms in the regulations and regulatory documents that relate to "safety classification" of components. They often have specific meaning that might not be intuitive. The goal of this appendix is to show this specificity, as well as to highlight the variety of terms used in regulatory space to discuss safety classification.

In the regulatory space, the term "safety-related" applies to SSCs, procedures, and controls (of a facility or process) that are relied upon to remain functional during and following design-basis accidents. These design basis accidents have been historically performed as part of a deterministic safety analysis. The functionality of safety-related SSCs ensures that key regulatory criteria, such as levels of radioactivity released, are met. Interestingly, there are very few places in the regulations that the term is used, let alone defined.

A.2 Safety-related – Code of Federal Regulations

A.2.1 10 CFR 50.2 – Definitions

The traditional (i.e., large light water reactor) definition of safety-related SSCs is contained in 10 CFR 50.2 and is as follows:

> Safety-related structures, systems and components means those structures, systems and components that are relied upon to remain functional during and following design basis events to assure:
>
> (1) The integrity of the reactor coolant pressure boundary
>
> (2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
>
> (3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable.

In addition, "safety-related" is used, but not defined, in the context of the definition of a basic component, as follows:

> In all cases, *basic component* includes **safety related design, analysis, inspection, testing, fabrication, replacement parts, or consulting services** that are associated with the component hardware, whether these services are performed by the component supplier or other supplier.

Finally, 10 CFR 50.2 uses, but does not define, "safety-related" in the context of construction, as follows:

> Construction or constructing means, for the purposes of § 50.55(e), the analysis, design, manufacture, fabrication, quality assurance, placement, erection, installation, modification, inspection, or testing of a facility or activity which is subject to the regulations in this part and consulting services related to the **facility or activity that are safety related**.

Ultimately, "safety-related" is only defined in the context of a safety-related SSC.

A.2.2 10 CFR 50.49 – Environmental qualification for electric equipment important to safety for nuclear power plants

This regulation uses and defines what constitutes safety-related electric equipment and also mixes the use of "safety-related" and "important to safety." Specifically, used in 10 CFR 50.49(b) in the following way:

> (b) Electric equipment important to safety covered by this section is:
>
> (1) **Safety-related electric equipment**.[3]
>
> (i) This equipment is that relied upon to remain functional during and following design basis events to ensure—
>
> (A) The integrity of the reactor coolant pressure boundary;
>
> (B) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
>
> (C) The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the guidelines in § 50.34(a)(1), § 50.67(b)(2), or § 100.11 of this chapter, as applicable.
>
> (ii) Design basis events are defined as conditions of normal operation, including anticipated operational occurrences, design basis accidents, external events, and natural phenomena for which the plant must be designed to ensure functions (b)(1)(i)(A) through (C) of this section.
>
> (2) Nonsafety-related electric equipment whose failure under postulated environmental conditions could prevent satisfactory accomplishment of safety functions specified in subparagraphs (b)(1) (i) (A) through (C) of paragraph (b)(1) of this section by the **safety-related** equipment.
>
> (3) Certain post-accident monitoring equipment.

The footnote in 10 CFR 50.49(b)(1) is of importance and states the following:

> Safety-related electric equipment is referred to as "Class 1E" equipment in IEEE 323–1974. Copies of this standard may be obtained from the Institute of Electrical and Electronics Engineers, Inc., 345 East 47th Street, New York, NY 10017.

It's important to note that the regulation references an IEEE standard that is written in the context of large light water reactors and has not been historically used by smaller reactor designs (e.g., research and test reactors, nonpower reactors).

A.2.3 10 CFR 50.55a – Codes and standards

The term "safety-related" is used, but not defined, in the context of in-service testing requirements for pre-1971 plants (10 CFR 50.55a(f)(1)).

A.2.4 10 CFR 50.65 – Requirements for monitoring the effectiveness of maintenance at nuclear power plants

The term "safety-related" is used, but not defined (the 10 CFR 50.2 definition is largely used), in the context of SSCs that should be monitored in terms of maintenance, as follows:

> (b) The scope of the monitoring program specified in paragraph (a)(1) of this section shall include **safety related** and nonsafety related structures, systems, and components, as follows:
>
> (1) **Safety-related** structures, systems and components that are relied upon to remain functional during and following design basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable to the guidelines in Sec. 50.34(a)(1), Sec. 50.67(b)(2), or Sec. 100.11 of this chapter, as applicable.
>
> (2) Nonsafety related structures, systems, or components:
>
> (i) That are relied upon to mitigate accidents or transients or are used in plant emergency operating procedures (EOPs); or
>
> (ii) Whose failure could prevent **safety-related** structures, systems, and components from fulfilling their **safety-related** function; or
>
> (iii) Whose failure could cause a reactor scram or actuation of a safety-related system.

A.2.5 10 CFR 50.69 – Risk-informed categorization and treatment of structures, systems, and components for nuclear power reactors

Section 50.69 to 10 CFR proposes an alternate categorization of SSCs, which has not yet been used for a new light water or nonlight water reactor, and is the following:

> (a) *Definitions*.
>
> *Risk-Informed Safety Class (RISC)–1* structures, systems, and components (SSCs) means **safety-related** SSCs that perform safety significant functions.

> *Risk-Informed Safety Class (RISC)–2* structures, systems and components (SSCs) means nonsafety-related SSCs that perform safety significant functions.
>
> *Risk-Informed Safety Class (RISC)–3* structures, systems and components (SSCs) means safety-related SSCs that perform low safety significant functions.
>
> *Risk-Informed Safety Class (RISC)–4* structures, systems and components (SSCs) means nonsafety-related SSCs that perform low safety significant functions.
>
> *Safety significant function* means a function whose degradation or loss could result in a significant adverse effect on defense-in-depth, safety margin, or risk.

A.2.6 10 CFR Part 50, Appendix B – Quality assurance criteria for nuclear power plants and fuel reprocessing plants

Applicability of this appendix is straightforward, as the regulation states the following:

> The pertinent requirements of this appendix apply to all activities affecting the **safety-related** functions of those structures, systems, and components; these activities include designing, purchasing, fabricating, handling, shipping, storing, cleaning, erecting, installing, inspecting, testing, operating, maintaining, repairing, refueling, and modifying.

A.2.7 10 CFR Part 50, Appendix R – Fire protection program for nuclear power facilities operating prior to January 1, 1979

Generally, Appendix R to 10 CFR Part 50 does not apply to new plants. Interestingly, the regulation makes the assertion that some of these terms are used interchangeably, stating the following, "…The phrases 'important to safety,' or '**safety-related**,' will be used throughout this Appendix R as applying to all safety functions. The phrase 'safe shutdown' will be used throughout this appendix as applying to both hot and cold shutdown functions."

A.2.8 10 CFR 51.4 – Definitions

This section defines construction in the context of safety-related activities as follows:

> (1) For production and utilization facilities, the activities in paragraph (1)(i) of this definition, and does not mean the activities in paragraph (1)(ii) of this definition.
>
> > (i) Activities constituting construction are the driving of piles, subsurface preparation, placement of backfill, concrete, or permanent retaining walls within an excavation, installation of foundations, or in-place assembly, erection, fabrication, or testing, which are for:

(A) **Safety-related** structures, systems, or components (SSCs) of a facility, as defined in 10 CFR 50.2;

(B) SSCs relied upon to mitigate accidents or transients or used in plant emergency operating procedures;

(C) SSCs whose failure could prevent safety-related SSCs from fulfilling their **safety-related** function;

(D) SSCs whose failure could cause a reactor scram or actuation of a **safety-related** system;

(E) SSCs necessary to comply with 10 CFR part 73;

(F) SSCs necessary to comply with 10 CFR 50.48 and criterion 3 of 10 CFR part 50, appendix A; and

(G) Onsite emergency facilities (*i.e.*, technical support and operations support centers), necessary to comply with 10 CFR50.47 and 10 CFR part 50, appendix E.

A.2.9 10 CFR 73.22 – Protection of safeguards information: specific requirements

This regulation is specific to what must be protected as safeguards information and uses, but does not define the term "safety-related," as follows:

(1) Physical Protection. Information not classified as Restricted Data or National Security Information related to physical protection, including:

(i) The composite physical security plan for the facility or site;

(ii) Site-specific drawings, diagrams, sketches, or maps that substantially represent the final design features of the physical security system not easily discernible by members of the public;

(iii) Alarm system layouts showing the location of intrusion detection devices, alarm assessment equipment, alarm system wiring, emergency power sources for security equipment, and duress alarms not easily discernible by members of the public;

(iv) Physical security orders and procedures issued by the licensee for members of the security organization detailing duress codes, patrol routes and schedules, or responses to security contingency events;

(v) Site-specific design features of plant security communications systems;

(vi) Lock combinations, mechanical key design, or passwords integral to the physical security system;

> (vii) Documents and other matter that contain lists or locations of certain **safety-related** equipment explicitly identified in the documents or other matter as vital for purposes of physical protection, as contained in security plans, contingency measures, or plant specific safeguards analyses;

A.2.10 10 CFR 73.54 – Protection of digital computer and communication systems and networks

This regulation uses, but does not define, the term "safety-related," in the context of what is commonly referred to as "critical digital assets" (not defined in 10 CFR 73.54), as follows:

> (a) Each licensee subject to the requirements of this section shall provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1.
>
> (1) The licensee shall protect digital computer and communication systems and networks associated with:
>
> (i) **Safety-related** and important-to-safety functions…

A.2.11 10 CFR 100.23 – Geologic and seismic siting criteria

In the context of remote "safety-related building" siting, this regulation uses, but does not define the term, as follows:

> Determination of siting factors for other design conditions. Siting factors for other design conditions that must be evaluated include soil and rock stability, liquefaction potential, natural and artificial slope stability, cooling water supply, and remote **safety-related** structure siting. Each applicant shall evaluate all siting factors and potential causes of failure, such as, the physical properties of the materials underlying the site, ground disruption, and the effects of vibratory ground motion that may affect the design and operation of the proposed nuclear power plant.

A.2.12 10 CFR Part 100, Appendix A – Seismic and geologic siting criteria for nuclear power plants

This term is used in the context of siting safety-related structures, also does not apply to new reactors.

A.2.13 Applicable regulations that are related to design or analysis of reactors

A.2.13.1 10 CFR 1.13 – Advisory Committee on Reactor Safeguards

In the context of what the ACRS is allowed to review:

> The Committee, on its own initiative, may conduct reviews of specific generic matters or nuclear facility **safety-related** items.

A.2.13.2 10 CFR 22.2 Scope

In the context of the applicability of 10 CFR Part 21, "Reporting of defects and noncompliance," the term is used but not defined:

> (d) Nothing in these regulations should be deemed to preclude either an individual, a manufacturer, or a supplier of a commercial grade item (as defined in § 21.3) not subject to the regulations in this part from reporting to the Commission, a known or suspected defect or failure to comply and, as authorized by law, the identity of anyone so reporting will be withheld from disclosure. NRC regional offices and headquarters will accept collect telephone calls from individuals who wish to speak to NRC representatives concerning nuclear **safety-related** problems…

A.2.13.3 10 CFR 21.3 Definitions

In terms of how "basic component" is defined under 10 CFR 21.3(4):

> (4) In all cases, basic component includes **safety-related** design, analysis, inspection, testing, fabrication, replacement of parts, or consulting services that are associated with the component hardware, design certification, design approval, or information in support of an early site permit application under part 52 of this chapter, whether these services are performed by the component supplier or others.

In the context of construction (similar to 10 CFR 51.4):

> *Constructing* or *construction* means the analysis, design, manufacture, fabrication, placement, erection, installation, modification, inspection, or testing of a facility or activity which is subject to the regulations in this part and consulting services related to the facility or activity that are **safety related**.

In the context of operation in the scope of the licensed activity:

> *Operating or operation* means the operation of a facility or the conduct of a licensed activity which is subject to the regulations in this part and consulting services related to operations that are **safety related**.

In the context of SSCs:

> ***Safety-related** structures, systems, and components (SSCs)* mean, for the purposes of this part, those structures, systems, and components that are relied on to remain functional during and following design basis events to ensure the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor and maintain it in a safe shutdown condition, or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposure comparable to the guidelines in 10 CFR 50.34(a)(1).

A.2.14 Not applicable regulations

A.2.14.1 10 CFR Part 32 – Specific Domestic Licenses to Manufacture or Transfer Certain Items Containing Byproduct Material

Defined in 10 CFR 32.15(a) in the following way for an individual licensed under 10 CFR 32.14:

> (1) Maintain quality assurance systems in the manufacture of the part or product, or the installation of the part into the product, in a manner sufficient to provide reasonable assurance that the **safety-related** components of the distributed products are capable of performing their intended functions

Additionally in 10 CFR 32.55 in the following way:

> (b) Each person licensed under § 32.53 shall:
>
> > (1) Maintain quality assurance systems in the manufacture of the luminous safety device in a manner sufficient to provide reasonable assurance that the safety-related components of the distributed devices are capable of performing their intended functions…

Finally in 10 CFR 32.62 as follows:

> (c) Each person licensed under § 32.61 shall:
>
> > (1) Maintain quality assurance systems in the manufacture of the ice detection device containing strontium-90 in a manner sufficient to provide reasonable assurance that the safety-related components of the distributed devices are capable of performing their intended functions

A.3 Safety-related – NRC glossary

Defined slightly differently from 10 CFR 50.2 as follows:

> In the regulatory arena, this term applies to systems, structures, components, procedures, and controls (of a facility or process) that are relied upon to remain functional during and following design-basis events. Their functionality ensures that key regulatory criteria, such as levels of radioactivity released, are met. Examples of **safety-related** functions include shutting down a nuclear reactor and maintaining it in a safe-shutdown condition.

A.4 Safety-related – Licensing Modernization Project

Recently, risk-informed guidance, such as RG 1.233, "Guidance for a Technology-Inclusive, Risk-Informed, and Performance-Based Methodology to Inform the Licensing Basis and Content of Applications for Licenses, Certifications, and Approvals for Non-Light-Water Reactors," Revision 0, issued June 2020, has defined safety-related as those components that are relied upon for licensing basis events to remain within the frequency-consequence curve or those components that prevent beyond design basis events from carrying consequences larger than the 10 CFR 50.34 limits (i.e., 25 rem).

The definition of safety-related in RG 1.233 appears as the following:

> SSCs selected by the designer from the SSCs that are available to perform the required safety functions to mitigate the consequences of design basis events (DBEs) to within the LBE Frequency-Consequence evaluation target (F-C target), and to mitigate design basis accidents (DBAs) that only rely on the SR SSCs to meet the dose limits of 10 CFR 50.34 using conservative assumptions.

The term is also defined using an "or" logic operator in the following way:

> SSCs selected by the designer and relied on to perform required safety functions to prevent the frequency of beyond design basis events (BDBE) with consequences greater than the 10 CFR 50.34 dose limits from increasing into the DBE region and beyond the F-C target.

Interestingly the LMP classification scheme focuses on mitigation of events, instead of prevention, which is closer to the majority focus of 10 CFR 50.2 definition. The LMP classification scheme is component-focused and not functionally-focused.

A.5 Important to safety – Code of Federal Regulations

Generally this term comes from the general design criteria, as defined in Appendix A to 10 CFR Part 50. Often a term used arbitrarily in the regulatory space, which implies some safety-relation of a component. This has been a long-standing understood point of confusion, not just between the NRC staff themselves, but also between the NRC staff and their external stakeholders (i.e., the public, the industry).

Important to safety SSCs are those safety-related and non-safety related SSCs whose function is to protect the health and safety of the public. Safety-related SSCs are those important to safety SSCs that perform one of three important safety functions, as defined in 10 CFR 50.2 [2].

There are two areas where "important to safety" SSCs are mentioned in the regulations: in Appendix A to 10 CFR Part 50 and in Appendix A to 10 CFR Part 100.

A.5.1 10 CFR Part 50 – Domestic Licensing of Production and Utilization Facilities

This term is loosely defined in 10 CFR Part 50, Appendix A as follows:

> The principal design criteria establish the necessary design, fabrication, construction, testing, and performance requirements for structures, systems, and components important to safety; that is, structures, systems, and components that provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the public.

Consistent with 10 CFR Part 50, Appendix A, GDC 2, "Design bases for protection against natural phenomena," important to safety SSCs should be designed to remain functional following a safe shutdown earthquake. The application of seismic qualification methods other than dynamic analysis or testing require technical justification and review by the NRC staff.

Consistent with 10 CFR Part 50, Appendix A, GDC 1, "Quality standards and records," important to safety SSCs should be designed, constructed and tested to appropriate quality standards commensurate with their safety function. Industrial standards supplemented by augmented requirements such as rigorous analysis, NDE, testing and QA as determined by the reliability and availability controls [2]. A functional definition of these SSCs "important to safety" or "safety related" is found in 10 CFR Part 100, Appendix A.

A.5.2 10 CFR Part 100 – Reactor Site Criteria

Important to safety SSCs are defined in 10 CFR Part 100, Appendix A, Section I, "Purpose," as those SSC that are designed "to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions."

Within the definition of "Safe Shutdown Earthquake," which is contained in Section III, "Definitions," to Appendix A of 10 CFR Part 100, these important to safety SSCs are discussed as those that remain functional throughout the event:

> (c) The Safe Shutdown Earthquake is that earthquake which is based upon an evaluation of the maximum earthquake potential considering the regional and local geology and seismology and specific characteristics of local subsurface material. It is that earthquake which produces the maximum vibratory ground motion for which certain structures, systems, and components are designed to remain functional. These structures, systems, and components are those necessary to assure:
>
> (1) The integrity of the reactor coolant pressure boundary,
>
> (2) The capability to shut down the reactor and maintain it in a safe shutdown condition, or
>
> (3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the guideline exposures of this part.

A.6 Safety-significant

Usually terms that are used in risk-informed regulation or guidance, such as 10 CFR 50.69 or RG 1.233. For 10 CFR 50.69, there are four specific "RISC" categories, and safety-significant is a term that is used throughout. For RG 1.233, safety-significant encapsulates components that are safety-related and nonsafety-related with special treatment.

A.6.1 Safety-significant – NRC Glossary

This term is defined in the NRC glossary as follows, "When used to qualify an object, such as a system, structure, component, or accident sequence, this term identifies that object as having an impact on safety, whether determined through risk analysis or other means, that exceeds a predetermined significance criterion."

A.6.2 Safety-Significant – RG 1.233

Safety-significant is a term defined in the LMP SSC and DID papers. All safety-significant SSCs are either classified as safety-related or NSRST. These components are either risk-significant or required for defense-in-depth. These safety-significant SSCs are subject to special treatment requirements. These requirements always include specific performance requirements to provide adequate assurance that the SSCs will be capable of performing their functions with significant margins and with a high degree of reliability. These include numerical targets for SSC reliability and availability, design margins for performance of essential safety functions, and monitoring of performance against these targets with appropriate corrective actions when targets are not fully realized.

A.7 Nonsafety-related

Components in the plant that have no safety classification (i.e., no special treatment).

A.8 Nonsafety-related with special treatment

Often referred to by its acronym – NSRST – and largely comes from risk-informed guidance. These are components in the plant that are not relied upon, in deterministic analyses, to remain functional during design basis accidents, but do have certain special treatment applied (e.g., quality assurance, testing requirements). Most used in risk-informed performance-based guidance and are often defined as components that perform risk-significant functions or functions necessary to assure defense-in-depth.

A.9 Special treatment

The purpose of special treatment is discussed in RG 1.201, "Guidelines for Categorizing Structures, Systems, and Components in Nuclear Power Plants According to Their Safety Significance," Revision 1, issued May 2009, in the following way:

> …special treatment refers to those requirements that provide increased assurance beyond normal industrial practices that structures, systems, and components (SSCs) perform their design-basis functions.

Special treatment requirements are typically defined as those requirements that exceed normal commercial and industrial practices to provide a greater degree of confidence in the capability of structures, systems and components (SSCs) to perform their safety functions under the design-basis conditions throughout their service life. Special treatment requirements encompass such aspects as quality assurance (QA), environmental and seismic qualification, inspection and testing and performance monitoring.

This term evolved from GDC 1 and 2 to resolve the confusion between "safety-related" and "important to safety." The way SSCs have been categorized as safety-related or important to safety has historically been based on deterministic analysis and engineering judgement. This issue evolved into the application of the terms: special treatment, graded QA, regulatory treatment of non-safety systems (RTNSS), and the 10 CFR 50.69 risk categorization rulemaking.

A.10 Graded QA or graded requirements

This term was used before the development of RTNSS. Nevertheless, the process to identify risk significant SSCs later became the basis for 10 CFR 50.69. SECY 95-059 was referenced but could not be found on the NRC's publicly available documents.

This process is a voluntary alternative to 10 CFR Part 50, Appendix B, that applied to operating plants; there were several pilot programs initiated. This term was developed because the NRC determined that certain nonsafety-related SSCs warrant some QA treatment. RG 1.201, RG 1.176, and NUREG/CR-6752 offer some guidance on this.

A.11 Regulatory treatment of nonsafety systems

Often referred to by its acronym – RTNSS – and commonly associated with passive plants. Components that have the RTNSS designation typically are nonsafety-related but perform risk-significant functions. The five criteria associated used to determine if components should be treated under RTNSS are those components (1) that are relied upon for beyond design basis NRC-required performance requirements (i.e., ATWS or SBO), (2) that ensure long-term safety (i.e., period after 72 hours), (3) relied upon to meet the Commission goals, (4) needed to function to meet the containment goals during severe accidents, and (5) that prevent the interaction between passive safety systems and active nonsafety components.

A.12 Nonsafety-related with no special treatment (NST)

NST is defined by the LMP SSC paper as those SSCs that are not classified as safety-related or NSRST and therefore do not have any special treatment.

NSRST is defined in the LMP SSC paper as:

> Non-safety related SSCs relied on to perform risk significant functions. Risk significant SSCs are those that perform functions that prevent or mitigate any LBE from exceeding the F-C target, or make significant contributions to the cumulative risk metrics selected for evaluating the total risk from all analyzed LBEs.
>
> Or
>
> Non-safety related SSCs relied on to perform functions requiring special treatment for DID adequacy.

Both of these definitions are related to the F-C curve. These NSRST SSCs fall at a certain distance away from what is called the "ISO Part 20 line."

A.13 Risk-significant

As defined in the NRC's glossary, risk-significant, "can refer to a facility's system, structure, component, or accident sequence that exceeds a predetermined limit for contributing to the risk associated with the facility. The term also describes a level of risk exceeding a predetermined "significance" level."' Additionally, risk-significant components have been defined in risk-informed guidance to meet more specific risk criteria.

Risk-significant SSCs include those SSCs that are required to function post-accident for 72 hours. Risk-significant SSCs also include those SSCs that accomplish defense in depth functions and limit challenges to safety-related systems [2].

A.14 Safety grade

To a lesser extent, the non-regulatory term "safety grade" is part of the confusion regarding the multiple terms that concern safety classification of SSCs. Safety grade is commonly regarded as being synonymous with "safety related" and "important to safety." [3]

A.15 10 CFR 50.69 safety classes

Section 50.69, "Risk-informed categorization and treatment of structures, systems and components for nuclear power reactors," to 10 CFR describes a risk-informed categorization scheme for SSCs. SSCs are broken down into four categories as per 10 CFR 50.69(a):

- Risk-Informed Safety Class (RISC)–1 structures, systems, and components (SSCs) means safety-related SSCs that perform safety significant functions.
- Risk-Informed Safety Class (RISC)–2 structures, systems and components (SSCs) means nonsafety-related SSCs that perform safety significant functions.
- Risk-Informed Safety Class (RISC)–3 structures, systems and components (SSCs) means safety-related SSCs that perform low safety significant functions.
- Risk-Informed Safety Class (RISC)–4 structures, systems and components (SSCs) means nonsafety-related SSCs that perform low safety significant functions.

This categorization is also shown in Figure A-1 [4].

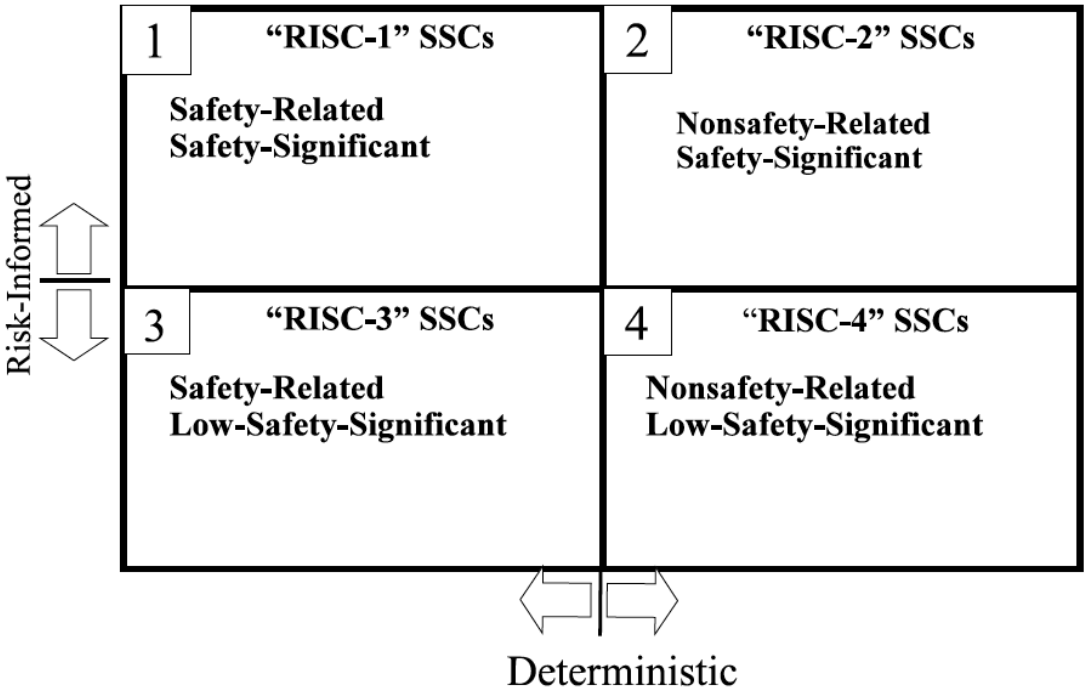

Figure A-1. RISC 1-4 from RG 1.201

APPENDIX B: EXAMPLE APPLICATION OF METHODOLOGY

This appendix provides one example application of the safety analysis MCA methodology, specifically with regard to the Aurora reactor. The purpose of this appendix is to both provide an example of the application of safety analysis methodology and to provide more information on how the methodology was applied to the Aurora and subsequently described in the Aurora combined license application, submitted in March 2020. This appendix does not describe the full extent of the analysis provided in the combined license application but only provides more context to the process under which the analysis was applied.

B.1 Selection of MCA

The first step in this methodology is to perform a thorough review of all possible events. This evaluation included the review of an exhaustive list of events, including all of the following types of resources:

- Generic events to all nuclear reactors
- Light water reactor events
- Reactor events, operating experience, and analytical methods for advanced reactors of similar design (fuel type, size, etc.)
    - Metal-fueled fast reactor events and operating experience
    - Compact reactor operating experience and analytical methods
- Expert opinion on similar conceptual designs

From this large list of events, the criteria within this methodology were applied to down select further. First, the events were screened for applicability, as per Criterion 1. Events that were found to be inapplicable were not further analyzed. For example, the Aurora safety analysis did not consider main steam line break events since there is no water in the system; this event was screened out of the safety analysis by Criterion 1. Second, the events that passed Criterion 1 were screened under Criterion 2 for credibility. Events that were found to be incredible were not further analyzed. For example, the Aurora control drum malfunctions were limited to those malfunctions that are mechanically possible by the system; control drum malfunction events considering rotation rates that are larger than what is possible in the Aurora system were not further analyzed.

The events considered for the Aurora were grouped according to phenomenology, as per the safety analysis methodology. The goal of this grouping is to reduce the analytical burden with the optionality of subsequently performing bounding analyses. The grouping of events resulted in "event groups," largely binned by common phenomena.

Within each event group, a bounding event was identified. This bounding event was then used to conservatively analyze the effects of the entire event group. In certain event groups, an even more limiting bounding event was selected, which was not an outcome of Criteria 1 or 2 of the methodology, in order to reduce the analytical burden. For example, for the positive reactivity insertion events, the bounding event assumed was control drum malfunctions that were more severe than that which was postulated; this was done in order to reduce the analytical space,

through the application of conservative assumptions. During this bounding analysis step, most event groups clearly were not challenging to the Aurora reactor or were able to be scoped under more challenging event groups.

The result of the down selection, even grouping, and bounding analysis was ultimately four event groups:

1. Increase of heat removal by secondary
2. Decrease of heat removal by secondary
3. Decrease of heat removal by heat pipes
4. Reactivity anomalies

Each of these four event groups has its own bounding analysis. Ultimately, the two overarching bounding events for the Aurora were determined to be the transient overpower event, which resulted from the reactivity anomalies event group, and the loss of heat sink event, which resulted from the decrease of heat removal by the secondary event group. These events were further analyzed to better understand which event is more challenging to the Aurora reactor. In the Aurora safety analysis, defense-in-depth considerations were applied at this step, in order to be able to better understand the overall system response.

In the case of the Aurora reactor, these analyses resulted in a zero dose. Since the key acceptance criterion for the safety analysis relates to the resulting consequence of the event (i.e., dose consequence), the acceptance criterion was met. Nevertheless, the safety analysis methodology requires the selection of an MCA. Since both events resulted in no dose, they were further analyzed to understand which event challenged the system in a more extreme way. Ultimately, peak fuel temperatures were higher during the loss of heat sink event than the transient overpower event. Additionally, temperatures above steady-state values were experienced for longer durations during the loss of heat sink event than the transient overpower event. Therefore, the loss of heat sink event was considered the more challenging event and is designated as the MCA for the Aurora.

After the selection of the MCA, the Aurora was analyzed in the context of external events. The goal of this external hazards analysis was to determine if the MCA determination could be challenged. In other words, to determine if an external hazard could cause an event more challenging to the Aurora reactor than the loss of heat sink event (i.e., the MCA). The external hazards methodology is separate from this safety analysis methodology and documented in the Aurora combined license application. Ultimately, no external hazard was found to result in a more challenging state than the MCA.

B.2 Design basis summaries

Assumptions regarding component function and inherent feature performance are made throughout the design and safety analysis of the Aurora. These assumptions are important to ensuring that the safety analysis is upheld and ultimately that the as-built facility reflects the one that was analyzed. These component functions and inherent features are captured as design bases, and summarized in gray boxes in the NRC application. Therefore, higher quality requirements are applied to these assumptions, as per Part III of the QAPD.

Because of the extremely small radionuclide inventory of the Aurora, the simple design of the system, and the generally passive or inherent nature of the plant, the acceptance criterion of the safety analysis is met. Nevertheless, it is of interest to determine which functions or inherent features contribute to the safety analysis acceptance criterion being met. For the Aurora, the foundational reason lies with the small inventory of the reactor. As such, the first step in this portion of the Aurora analysis was to look at hypothetical radionuclide release from the fuel. There were several iterations and sensitivity analyses of these hypothetical analyses that simply assumed a radionuclide release from the fuel. All of these analyses were hypothetical and extreme. Regardless, none of them exceeded the acceptance criterion or were close to exceeding the acceptance criterion. Because no specific functions or inherent features were relied on in these analyses, and they nevertheless resulted in this large margin, further functional and inherent features analysis was not conducted for the Aurora and no functions or features were deemed safety-related.

For the Aurora, even though bounding hypothetical releases do not cause the safety analysis acceptance criterion to be exceeded, the safety goal is to control the release of radionuclides by maintaining fuel integrity, as the fuel is the only source of radionuclides. The safety goal relates to keeping temperatures below those at which fuel is anticipated to melt because the fuel significantly loses its capability to retain radionuclides. As such, even though the fuel is not considered safety-related, 10 CFR Part 50, Appendix B, quality requirements are applied to it. Specifically, these quality requirements are applied to certain fuel characteristics, which will be controlled under Part II of the QAPD. This elevated treatment is specifically noted in the design basis summary of the relevant design basis in the NRC application.