Maximum Credible Accident Methodology

July 2021

Oklo Inc., Non-proprietary

Revision 2

Table of contents

1 Purpose and scope **3**
2 Analysis approach **5**
3 Identification of possible events **7**
4 Determination of applicability **8**
5 Evaluating credibility of events **9**
6 Grouping of events **11**
7 Performing bounding analyses **12**
8 Selecting the MCA **14**
9 Applying the defense-in-depth consideration **15**
10 Inclusion of risk insights **17**
11 Conclusion **18**

1 Purpose and scope

The purpose of this document is to summarize the safety analysis methodology performed by Oklo Inc. (Oklo) for the licensing bases of its designs. Oklo is requesting U.S. Nuclear Regulatory Commission (NRC) review and approval of the methodology outlined in this report.

This methodology could be utilized by any NRC applicant for the safety analyses of their designs and is not limited to Oklo designs. These safety analyses do not cover external hazards and how the facility responds to those hazards. The results of the safety analyses demonstrate a response to challenging conditions that ensures adequate protection of the public is maintained during the facility lifecycle.

This methodology is used to guide event analyses broadly, ultimately resulting in the identification of a specific event, the maximum credible accident (MCA), which becomes the licensing basis event for the design. The concept of an MCA has roots to the beginning of U.S. nuclear regulation[1], and the concept has informed regulation to the present time. At the core of this concept is the idea of identifying a sufficiently bounding accident to represent a "credible" but conservatively bounding worst case scenario in terms of possible accident scenarios. The concept of a credible accident differs from a hypothetical accident, in that the MCA methodology is intended to identify credible bounding events in a systematic way instead of assuming a hypothetical worst case without consideration of applicable events and sufficiently bounding event propagation and outcomes.

It is worth noting that existing NRC regulations do not require the categorization of events into either design basis accidents or design basis events. Instead, the regulations require an evaluation of normal operations and transient conditions anticipated during the life of the facility and a presentation of design bases, which focus on the functionality of components and systems. This focus on design bases allows for design and analysis flexibility and even suggests a need for a methodology for identification of key events for novel plant designs. This methodology also captures the defense-in-depth principle long held by the NRC by incorporating a process of applying the most limiting single failure to the safety analysis.

The MCA methodology may be used as a stand-alone methodology for licensing basis event selection with application of defense-in-depth considerations. It also may be integrated with a performance-based licensing methodology[2] that uses the selected licensing basis event to systematically identify key functions and features of the design. Specifically, both methodologies are appropriate for use in the licensing of novel plant designs that typically rely on passive functions and inherent features to assure safety.[3] The performance-based licensing methodology then applies the appropriate regulatory controls to ensure that those functions and features are maintained throughout the facility lifecycle. The safety analysis results obtained from the MCA methodology can then be used to develop inputs to demonstrate compliance with

[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] Oklo prepared a companion topical report, "Performance-Based Licensing Methodology," for this purpose.

[3] When used in these methodologies, "functions" are usually passive or active (e.g., valve actuation, shutdown rod insertion) and "features" are typically inherent or intrinsic system characteristics (e.g., reactivity feedback, heat transfer properties, structural configurations).

NRC requirements for applications for advanced reactor design permits, certifications, and licenses.

2 Analysis approach

Oklo uses this 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 with respect to consequence, 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 focused analysis of the safety of the reactor:

1. Perform a literature review to understand the historical context and past challenges considered for relevant fission reactor systems, both those that have operated and those proposed.

2. In the context of these past events considered, determine which events are applicable for the reactor design, and which, if any, new events specific to the reactor design would be applicable.

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

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

5. Identify and analyze the bounding events in each category. 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.

6. 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.

7. Apply a defense-in-depth consideration by assuming a single additional failure, chosen to be the most limiting single failure at the time of the event, in addition to the MCA.

8. 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.

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. As part of the safety-by-design approach undertaken by Oklo, these steps can be completed iteratively during the design process, such that insights gained in the process of identifying the MCA can drive improvements to the design. At the conclusion of this iterative approach, a final MCA analysis is conducted, and the MCA is identified and evaluated.

Figure 2-1 presents a visual representation of the MCA analysis process. The steps outlined above are described in more detail in Sections 3 through 9. The MCA, combined with the additional single failure for defense-in-depth, is ultimately designated as the licensing basis event.

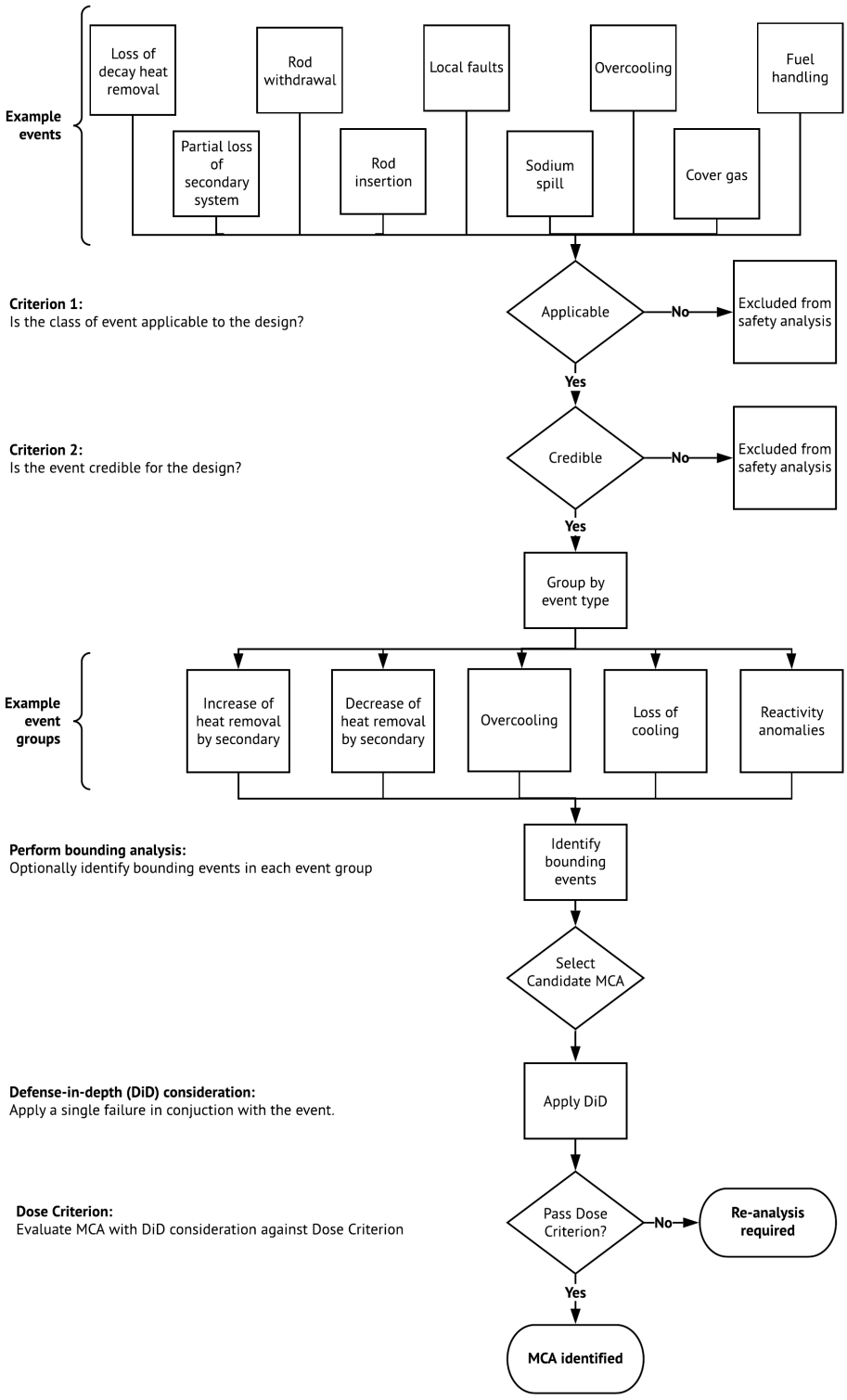

Figure 2-1: Visual representation of the event evaluation process

3 Identification of possible events

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

- Events generic 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 have the same relevance and importance. Reactor designs with similar design features are considered most closely, and their events are screened further, while reactor designs that are not sufficiently similar may receive less consideration. However, even for non-light water reactor designs, light water reactors have important operational experience and are a good candidate for event consideration regardless of design type.

This identification process systematically examines aspects of both operational and conceptual designs to ensure completeness in the event identification scope. Expert opinion is used to augment and challenge this process by providing additional perspective on novel or unique safety challenges associated with similar conceptual designs that may not be well characterized in existing literature or alternative resources.

During the event identification phase, all operating modes of the proposed reactor design are considered and evaluated such that the facility safety profile is sufficiently and comprehensively scoped. If there is ambiguity about the proper operating mode with which to associate an event based on the existing literature or expert opinions, justification for assignment of an event to an operating mode should be documented. The remainder of this methodology is directly utilized for all operating modes with no changes based on the operating mode being considered.

4 Determination of applicability

After all potential events are identified, a systematic process is used to screen the potential relevance of the identified events to the proposed design. Specifically, this screening process determines whether the event is applicable in terms of phenomenology. This determination is made utilizing 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 being reviewed. Events that are deemed applicable to the design under evaluation pass Criterion 1 and proceed for further evaluation.

Note that applicability screening entails the consideration of structures, systems, and components in the design in question, in this case the Oklo's design, that might provide similar or parallel functions to those events being screened. While events that include design aspects irrelevant to the design in question may be screened out, an alternative event that represents similar phenomenology (i.e., a "parallel event") may be added as an event to be considered for the applicability screening. 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 analyzed further. Events that do pass Criterion 1 continue through the safety analysis process. 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 would 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.
- Spurious movement of control rods would not be considered for a reactor that uses control drums instead of control rods for reactivity control during core life. Although this event would fail Criterion 1, a parallel event considering spurious control drum rotation would be considered and would be analyzed further.

5 Evaluating credibility of events

After Criterion 1 has been applied to the list of potential events, the events that met 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 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 are not mechanistically possible. It is different than Criterion 1 because the features analyzed do exist, and therefore the associated events have already been deemed applicable. Criterion 2A analyzes whether the events could occur in the reactor design under evaluation; the probability of the event occurring is not a consideration in this step. Criterion 2A requires that events are mechanistically possible, meaning that there must be a mechanism by which the event can occur in the system. For example, this criterion screens out events that are not physically possible and events that are precluded by the functional design of the system.

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 speed that is not physically 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 speed that is physically 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 all applicable and mechanistically possible single initiator events are systematically analyzed. As described in Section 3, events are considered for all operating modes. 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. It must be mechanistically possible that subsequent failure(s) could be caused by the single initiating event, and the entire event sequence must be mechanistically possible. The single initiator criterion, in combination with the allowance for the single initiator leading to a common set of failures, provides a generalized basis for scoping events typically associated with the design basis. Further detail on the process of event sequence

construction is outside of the scope of this document and is the responsibility of the designer to justify.

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. For example, an event where a single failure in the control drum motor could initiate a spurious rotation of a control drum would pass Criterion 2 and would be analyzed further. In contrast, if the system uses multiple controls drums that are electrically independent, a different event where one actuation system fails would not induce a rotation in all control drums, and therefore an event with all control drums spuriously operating would fail Criterion 2.

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 "applicable and credible" means that it has passed both Criterion 1 and Criterion 2. Applicable and credible events then proceed to be evaluated further.

6 Grouping of events

After the initial list of all potential events has been analyzed for applicability under Criterion 1, it is possible that many events remain. These events are then grouped into "event categories" to reduce the analytical burden. This grouping may 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 NRC applicant.

The grouping of events is a common practice in safety analysis for reactor designs and is intended to reduce the analytical burden. To continue the previous example, if control drums are used to control the reactivity of the plant, different manifestations of these malfunctions could be grouped as "reactivity insertion events" and "reactivity withdrawal events."

7 Performing bounding analyses

For those events that meet Criterion 2, the applicant conducts an analysis of the system response. Typically, the first step of the analysis is to identify a single bounding event from each event group, if appropriate. 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 bounding step is to reduce the overall analytical burden, since analysis of a conservatively large bounding event could encompass analyses of smaller (i.e., less challenging) events within the event group. Events are identified as bounding with respect to dose consequence. This identification may leverage engineering judgement or analysis, as appropriate. The rationale for utilizing a bounding approach by the applicant must be clearly justified and documented.

For example, a partial loss of electrical power could be bounded by an analysis that evaluates a full loss of electrical power if the consequence of that event is greater. This bounding analysis may be deemed appropriate through a combination of engineering judgement and analysis of the potential effects of a loss of electrical power and should be documented as such. Conducting this bounding analysis reduces the analytical burden of having to run multiple event analyses for different degrees of loss of electrical power which are otherwise subsumed in the bounding analysis.

Most events and bounded event groups are expected not to result in a dose consequence above the normal operation of the plant. For the events that have zero dose consequence, 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 applicable metric for measuring and ranking consequence is the offsite dose consequence, and therefore offsite dose consequence is the only acceptance criterion for the safety analyses described in this methodology. Specifically, this criterion is related to the regulatory limit for siting, in accordance with Title 10 of the *Code of Federal Regulations* (10 CFR) Part 100, "Reactor Site Criteria." It is referred to in this summary as the "Dose Acceptance Criterion," and is summarized in the box below. If the safety analysis for an event exceeds the Dose Acceptance Criterion, the methodology is terminated at this step and re-analysis must occur. This re-analysis may be the result of a change in design, or may be an analytical change within the evaluation. Ultimately, the design of the facility must be such that no events exceed this criterion. If the safety analysis passes the Dose Acceptance Criteria for all events, the process 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 TEDE.

8 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 from one design to another. In general, the event with the greatest dose consequence is selected as the MCA, but in the case that all analyzed events have zero dose consequence, or in the unlikely case that multiple events have the same dose consequence, this decision may consider other potential consequences, or even risk insights. Regardless, this step of the process should be thoroughly documented, including the identification of each event that is considered a candidate for the MCA and the justification by which the MCA is selected.

Note that external hazards are not considered as part of the down-selection process described in this MCA methodology, which is the process for evaluating internal events only. Nevertheless, external hazards are an important consideration in the licensing process. As such, after the MCA is selected, external hazards are analyzed against the design. If no external hazard is shown to be more challenging than the MCA, the MCA is upheld as chosen. If an external hazard or multiple external hazards are shown to be more challenging than the MCA, further action may need to be taken that could include re-analysis, design changes, further regulatory controls, or designating the external hazard as the MCA.[4]

[4] The detailed methodology for the analysis of external hazards is outside the scope of this summary. The Aurora at Idaho National Laboratory combined license application proposes one external hazards methodology, documented in Appendix A, "External hazards evaluation," to Chapter 1, "Site envelope and boundary," of Part II, "Final Safety Analysis Report."

9 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 as indicated by risk insights.

The following regulatory documents were reviewed in the drafting of this consideration:

- Appendix A, "General Design Criteria for Nuclear Power Plants," to 10 CFR Part 50
- Appendix K, "ECCS [emergency core cooling systems] Evaluation Models," to 10 CFR Part 50
- NEI 18-04, "Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development," Revision 1, issued August 2019
- Oklo Inc., "DG-1353 Pilot: Submittal to Support NRC Development and Implementation of DG-1353," September 2018
- Regulatory Guide 1.53, "Application of Single-Failure Criterion to Safety Systems," Revision 2, issued November 2003
- SECY 03-0047, "Policy Issues Related to Licensing Non-Light-Water Reactor Designs," issued May 28, 2003
- SECY 05-0138, "Risk-Informed and Performance-Based Alternatives to the Single-Failure Criterion," issued August 2, 2005
- SECY 05-0138, "Risk Informed and Performance-Based Alternatives to the Single-Failure Criterion, "issued August 2, 2005, Attachment 2, "Technical Work to Support Evaluation of a Broader Change to the Single-Failure Criterion"
- SECY 77-0439, "Single Failure Criterion," issued August 17, 1977

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 additional failure for the event, regardless of safety classification. Evaluating defense-in-depth across the whole design adds significantly increased levels of conservatism by considering design choices made on all components and ensuring all reasonable additional single failures are considered for their impact on the selected licensing basis event.

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. 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^{-4} per reactor year, as observed for design basis event analysis, but the threshold may be set to lower frequencies 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 modified in a manner that would ensure that the Dose Acceptance Criterion is met. If the criterion is met, the safety analysis is complete, and the final MCA has been identified and shown to be acceptable.

10 Inclusion of risk insights

Oklo uses probabilistic risk assessment to both confirm the MCA and apply defense-in-depth to its safety analyses, as described in Section 9. Ultimately, the methods used by Oklo for the safety analysis are largely deterministic. As such, limited information related to the methodology and implementation of probabilistic risk assessment is included in licensing applications. While risk insights are given a chapter of the license application as specified in the regulatory requirements for contents of the application, a risk assessment is not included, which is consistent with current and all historical licensing application precedent.

Oklo utilizes probabilistic risk insights in several ways during the design process of its facilities. One way Oklo uses these risk insights is to understand the reliability of its components; this information is solely for operational reliability, investment protection, and system performance and is therefore not included in a license application. Another way is to evaluate the results of the deterministic analysis by comparing them against the results of the probabilistic risk assessment. Since the regulatory requirements are simply to perform a probabilistic risk assessment and include the relevant results, license applications using this topical report methodology include a small subset of the probabilistic risk assessment performed on the facility that is relevant to the safety analysis. This approach is well suited for the safety case demonstration of first-of-a-kind reactors, for which sufficient operating experience may not exist to support a holistic probabilistic risk assessment. Over time, increased operating experience will inform improvements in the probabilistic risk assessment and the role of that analysis may be expanded, but the largely deterministic approach provides sufficient demonstration of adequate protection.

While this is not an exhaustive description of the application of risk insights, it is key to note that Oklo uses probabilistic risk assessment as a valuable tool, starting early in its iterative design process. Just as with analyses of normal and abnormal conditions, the use of risk insights can drive design changes, and in that case, the designer returns to previous steps and continues to iterate.

11 Conclusion

The methodology provided in this document is one way of systematically selecting a bounding event for the facility, which is designated the MCA, and becomes the licensing basis event. 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. 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 for 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. After the MCA is selected, external hazards are analyzed against the design to assure that the MCA is upheld.

Following the selection of the licensing basis event, a performance-based licensing methodology may be applied. The performance-based licensing methodology systematically identifies key functions and features of the design and applies the appropriate regulatory controls to ensure those functions and features are upheld throughout design, construction, and operation of the facility. These regulatory controls, including quality assurance measures, ensure that the safety functions are upheld and therefore that the assumptions and conclusions of the MCA analysis are valid. This performance-based licensing methodology, and associated classification methodology, is described in detail in Oklo's "Performance-Based Licensing Methodology Topical Report."