U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Public Meeting
Maximum Credible Accident Concept and Discussion

August 4, 2020

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Purpose

- The goal of this meeting is to:
  - Discuss background and context associated with event selection and assessment required by regulation
  - Provide feedback on the Maximum Credible Accident (MCA) approach proposed by the applicant
  - Begin aligning with Oklo on appropriate assumptions to be used in MCA/event assessment

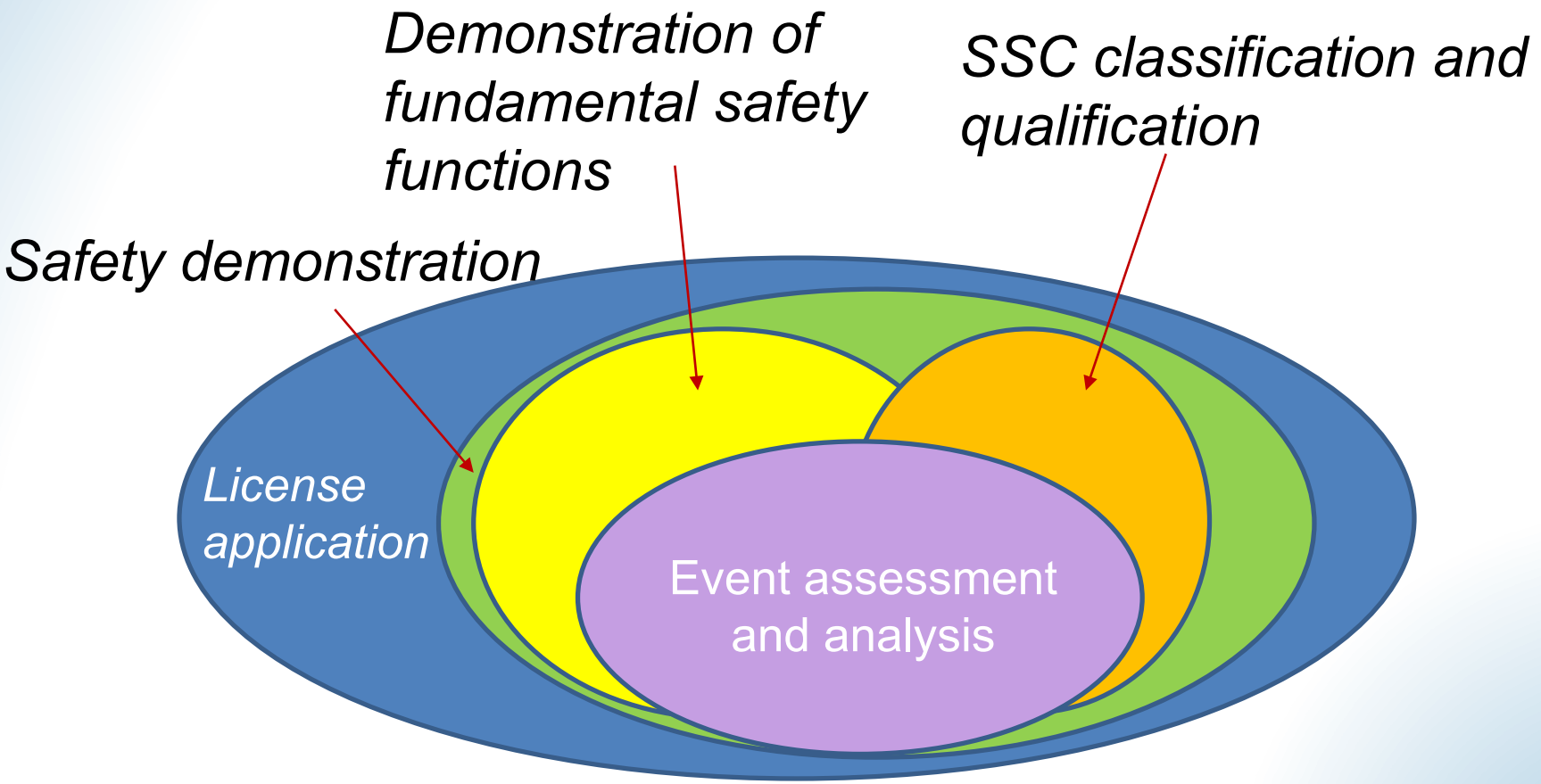
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Regulatory Basis

- 52.79(a) The final safety analysis report shall include the following information, at a level of information sufficient to enable the Commission to reach a final conclusion on all safety matters that must be resolved by the Commission before issuance of a combined license:
  - (a)(2) - A description and analysis of the structures, systems, and components of the facility with emphasis upon performance requirements, the bases, with technical justification therefor, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. It is expected that reactors will reflect through their design, construction, and operation an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products. The descriptions shall be sufficient to permit understanding of the system designs and their relationship to safety evaluations.

  - (a)(5) - An analysis and evaluation of the design and performance of structures, systems, and components with the objective of assessing the risk to public health and safety resulting from operation of the facility and including determination of the margins of safety during normal operations and transient conditions anticipated during the life of the facility, and the adequacy of structures, systems, and components provided for the prevention of accidents and the mitigation of the consequences of accidents.

Role of event assessment



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

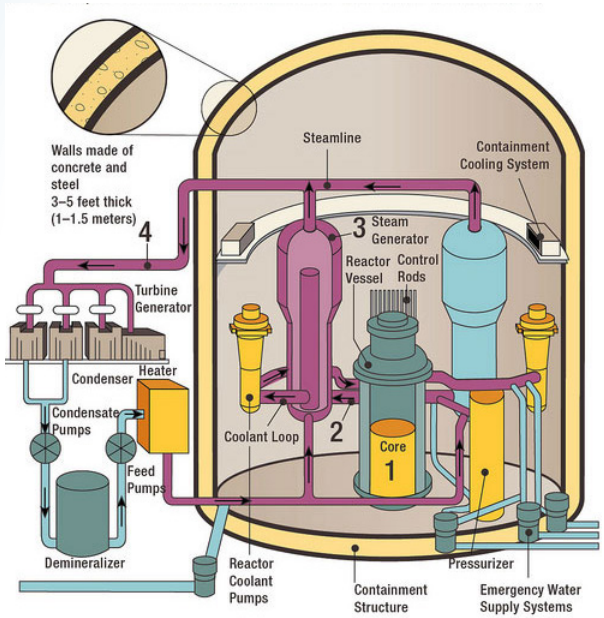
Event assessment provides a framework to evaluate risk

- It is not necessary to address each portion of the risk triplet equally as part of assessing and classifying events (events in this case, from the regulation: “normal operations and transient conditions anticipated during the life of the facility, and…prevention of accidents and the mitigation of the consequences of accidents”)
- Different approaches have been deemed acceptable in previous applications to address these regulatory requirements, and staff is receptive to further evolutions
- These approaches, discussed next, have emphasized diverse answers to the risk triplet in making a safety case

Context – Current means for event assessment (1)

- One means to address this requirement involves a traditional deterministic approach (using conservative analyses), supplemented by broader probabilistic considerations (best estimate with uncertainty)

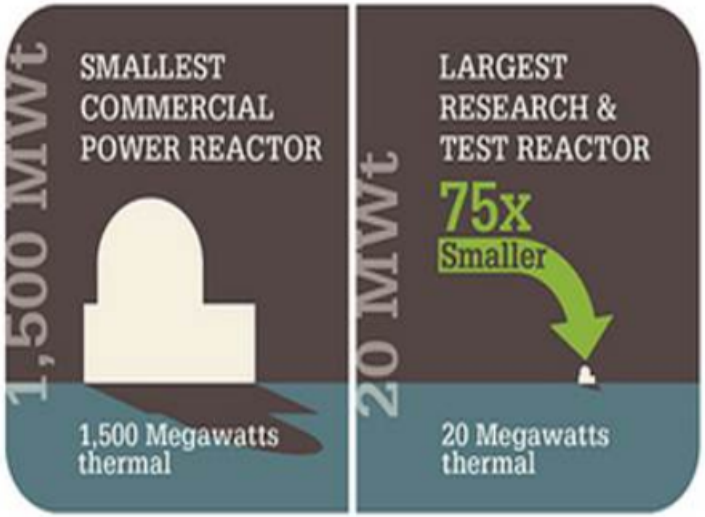
- This approach is reflected in current regulations and guidance



- Effectively, three key parts to safety case:
  - conservative safety analysis demonstrating that core damage is prevented in the case of design basis
  - demonstration that an event involving core damage with nominal barrier leakage will not cause doses at the EAB and LPZ distance in excess of 25 rem TEDE
  - Performance of a PRA that looks at entire plant design beyond the design basis to evaluate full event spectrum and, among other purposes, show Commission Safety Goal Policy is met

Context – Current means for event assessment (2)

- A second means that has been used is a Maximum Hypothetical Accident (MHA)
- This approach is used by non-power reactors, and is described in NUREG-1537 ("Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors")
- The MHA is an “incredible” event that bounds potential accidents



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Context – Current means for event assessment (3)

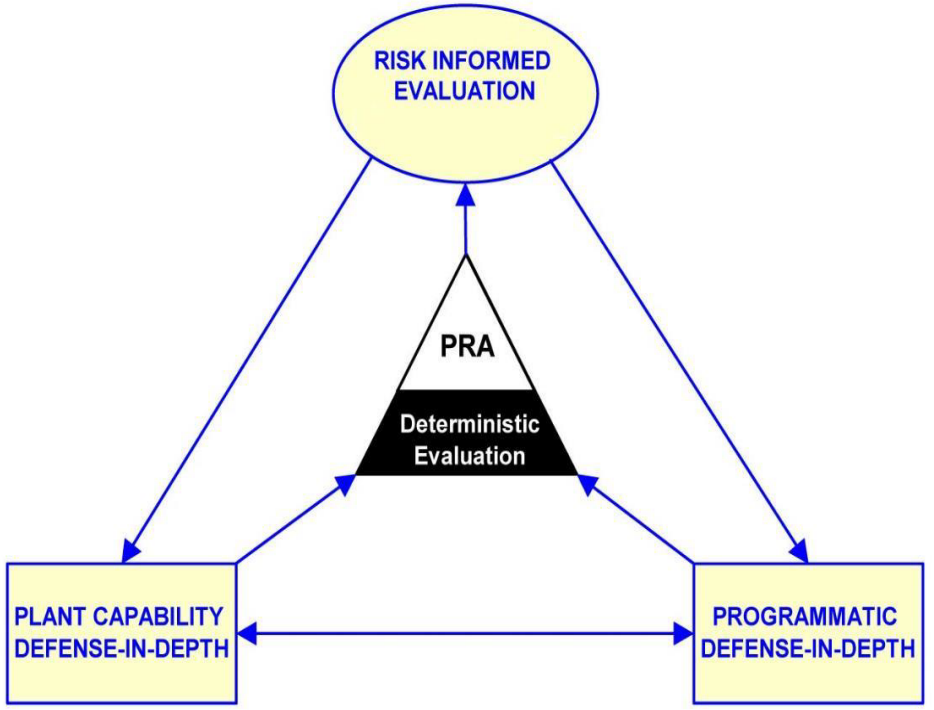
- Another approach that has recently been endorsed by the NRC (RG 1.233) is the Licensing Modernization Project (LMP):
  - Groups all event sequences based on frequency
  - Categorizes events to be considered in evaluating the design based on the frequency and consequences of each event sequence (including uncertainty when evaluating against the thresholds), with different acceptance criteria for each category

Modernization of Technical Requirements
for Licensing of Advanced Non-Light Water Reactors

Risk-Informed Performance-Based Guidance
for Non-Light Water Reactor Licensing Basis
Development

NRC staff finding and goal

- Staff recognizes these are not the only available approaches, but they provide a useful framework for understanding the safety finding the NRC staff must make to license a reactor design.
- Fundamentally, the NRC staff is looking to make a safety finding across a spectrum of operational and accident conditions
- Another consideration involved in making this finding involves evaluating defense-in-depth

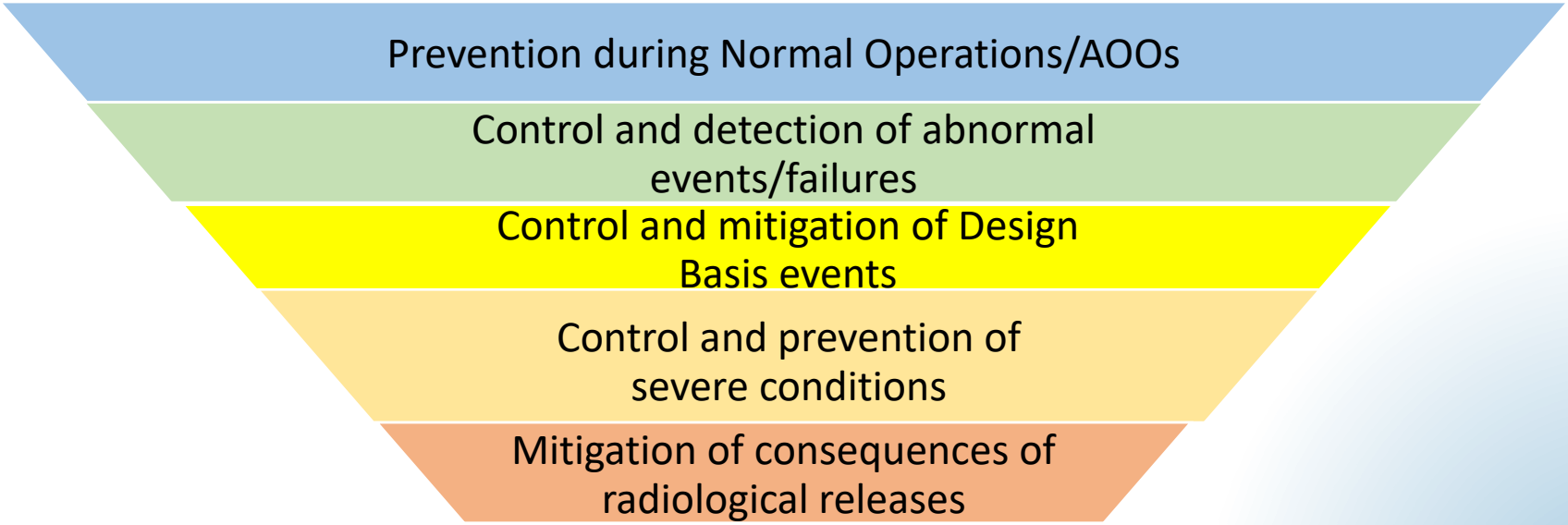


U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Defense-in-depth

- Defense-in-depth involves consideration of both prevention AND mitigation

- Implementing defense-in-depth involves evaluating the design as a whole (rather than just a single system or component) against a spectrum of events



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

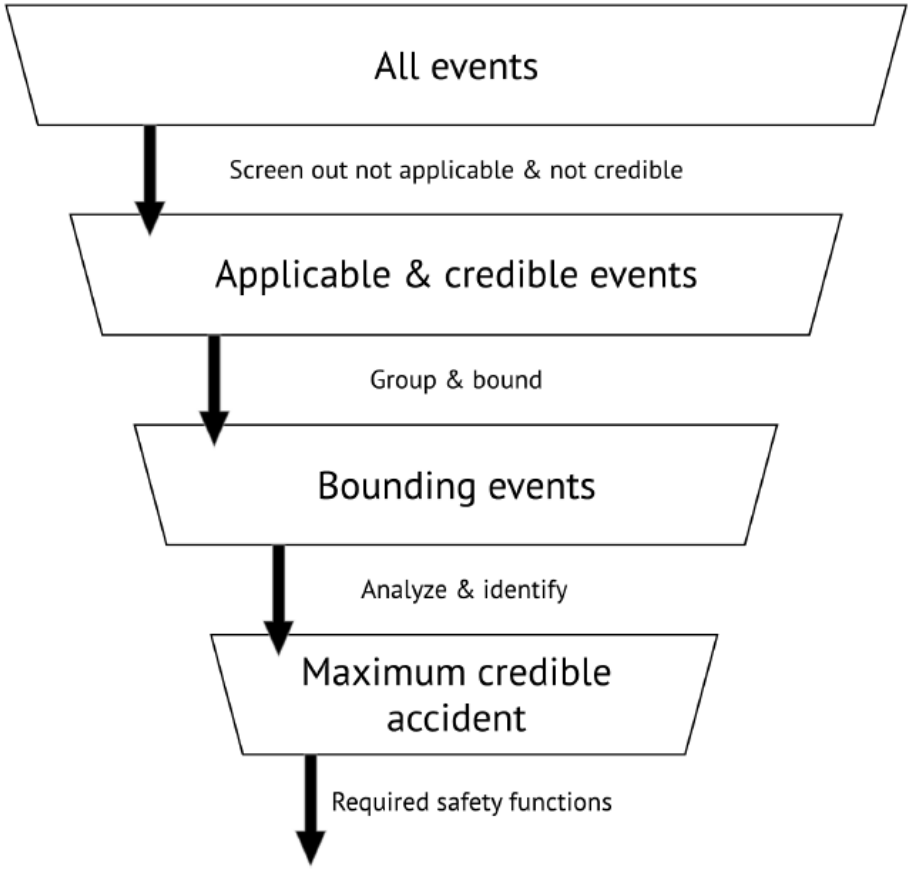
Defense-in-depth

- NRC policy on defense-in-depth – Excerpt from 60 FR 42622:

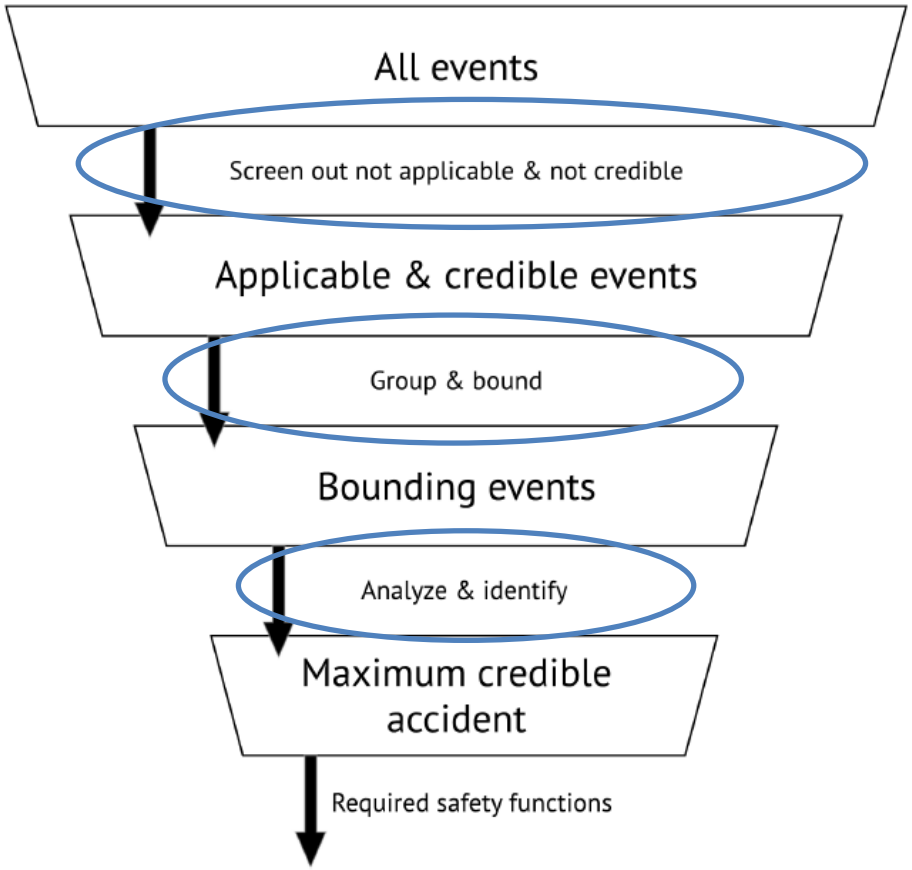
> "In the defense-in-depth philosophy, the Commission recognizes that complete reliance for safety cannot be placed on any single element of the design, maintenance, or operation of a nuclear power plant. Thus, the expanded use of PRA technology will continue to support the NRC's defense-in-depth philosophy by allowing quantification of the levels of protection and by helping to identify and address weaknesses or overly conservative regulatory requirements applicable to the nuclear industry. Defense-in-depth is a philosophy used by NRC to provide redundancy for facilities with "active" safety systems, e.g., a commercial nuclear power [facility], as well as the philosophy of a multiple-barrier approach against fission product releases."

MCA Approach in Aurora FSAR

- The MCA analysis approach described in FSAR Section 5.5 appears to be reasonable
  - Considers past challenges to fission reactor systems
  - Considers potentially new events specific to the Aurora



MCA Approach in Aurora FSAR



NRC staff needs additional information on the application of the MCA analysis approach as described in FSAR Sections 5.5 and 5.6

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

What could go wrong?

- Staff does not believe each of these requires the same level of discussion and documentation, but these issues are provided as a sample of areas requiring clarification within the proposed MCA:
  - The potential for a heat pipe failure (here, as an initiating event) with a failure to trip is not provided for in the FSAR
  - Dynamic effects associated with high energy rupture (secondary fluid) inside the module are not discussed
  - Additional justification is needed for not considering a cell can failure/leak over the life of the plant, and no provision is made for sampling/detection to ensure this assumption is valid
  - Many of the assumptions used to arrive at the proposed MCA rely on application of historical data and component usage that may not apply directly or be well-established for the usage case in the Oklo design
  - Components not identified in the FSAR but identified during staff audit could provide a potential path to the environment
  - External events and internal flooding and their effects on the safety of the reactor may require additional consideration and detail

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example – Unprotected heat pipe failure

- FSAR Section 2.7.2.7.2, “Heat pipe temperature sensors”
  Each heat pipe is instrumented with three thermocouples to provide redundancy. The thermocouples are located above the top of the reactor core in the heat exchanger region to reduce exposure to radiation.

- FSAR Section 2.7.3.4.2.1, “Heat pipe temperature fault signal”
  The fault signals are aggregated such that at least one of the following criteria must be met for each reactor cell heat pipe: (1) two or more direct temperature channels shall not be sending a fault signal […], or (2) one direct temperature channel and nine or more indirect temperature channels for a heat pipe with two failed sensors shall not be sending a fault signal.

- Oklo report, “Heat Pipe Failure in Aurora,” (examined during Audit)
  - Includes an analysis of single reactor cell

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Unprotected heat pipe failure How likely is it?

- It is NRC staff's current belief that a heat pipe degradation or failure should be considered as an anticipated occurrence for the Aurora design
  - Heat pipes are a relatively mature technology, however:
    1. The FSAR contains no references to reliability or lifetime data for the heat pipes used in the Aurora design
    2. There are examples where heat pipe degradation and failure has occurred even when mature heat pipe designs are used.
    3. Expert opinion is that heat pipe degradation and failure needs to be considered for heat pipe reactor designs (e.g., Kilopower and Megapower)
    4. Large number of heat pipes used in the Aurora design increases the likelihood of heat pipe failure during the life of the plant.
  - FSAR Section 5.5.1.2.3.2, "Aurora analysis [for an event similar to a decrease in reactor coolant system flowrate]," states that

    The only reasonable event in the decrease in heat removal by the heat pipes event category is a local fault where a single heat pipe experience an enclosure failure

Unprotected heat pipe failure Common cause failure

- NRC staff's research and consultation with experts in the field of heat pipe design and use identified that:
  - Heat pipe degradation and failure can occur in several manners
  - A spectrum of heat pipe degradation and failure scenarios should be considered (e.g., heat pipe operating at several different fractions of its expected performance)
- NRC staff's questions over the current design:
  - NRC staff is uncertain what temperature will be measured by the heat pipe sensing thermocouple under conditions of heat pipe degradation and/or failure
    - Uncertainty regarding specific location of heat pipe temperature sensing thermocouples
    - Consideration of a spectrum of heat pipe degradation scenarios
    - Potential for heat transfer from neighboring heat pipes and/or other hot surfaces may impact thermocouple hot junction
  - Has any work been done by Oklo or otherwise to physically validate the temperature measurement and aggregation methods (direct and indirect) described in FSAR Sections 2.7.2.7.2 and 2.7.3.4.2.1?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Unprotected heat pipe failure Reliability and OpE

- Separately, NRC staff questions the implied characterization of an unprotected heat pipe failure as being not credible
- NRC staff is aware of at least two instances of reactors using control rod designs similar to the Oklo Aurora design failing to insert upon demand (documented in NRC non-power reactor event report 54546, which occurred at the University of New Mexico AGN-201 reactor)
- The reactor trip system in the design is an "active" system, and could be subject to the potential for common cause failure, as described in the previous slides or other means, such as those experienced at the UNM reactor
- How is the NRC policy on defense in depth reflected by the use of a single active system to prevent fuel damage without providing for mitigation

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example - sCO_2 Pipe Rupture within Capsule or Module Shell

- FSAR Section 2.6.3 describes a heat exchanger system utilizing highly pressurized sCO_2
- NRC staff has questions about dynamic effects of a pipe rupture within the capsule or module shell
  - Over-pressurization and/or dynamic effects, including of the effects of pipe whipping, of a pipe rupture have the potential to:
    - Damage the capsule or module shell which serve as barriers to fission product release
    - Deform the shutdown rod insertion path
    - Damage to nearby structures due to pipe whip

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

How likely is it?

- The relative importance of this question depends on the approach taken:
  - For conservative, deterministic analysis, nothing may be needed
  - As acceptance criteria and inputs change based on the frequency, more rigor behind the frequency basis is needed
  - If frequency is being used as the primary argument to screen or omit events, a well-founded quantitative basis will generally be necessary
- With this understanding, the criteria for what constitutes “credible” needs clarification in the FSAR, and the basis for excluding certain events needs additional documentation

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

What are the consequences?

- At the present stage, this question is difficult to answer – the MCA provides for zero dose consequences, and does not clearly bound potential events like an MHA might

- If these examples or others are determined to be credible, additional evaluation will be needed to identify the consequences

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Staff questions on MCA approach as applied

- Additional information is needed on how the MCA approach applied by Oklo addresses the safety bases (as related to the risk triplet) in some ways.
  - Staff has identified potential gaps in the application and outcome of the Oklo MCA approach along with events that are not evaluated in the FSAR.
- Based on examples described, staff believes that it may be necessary to evaluate the release of radionuclides from the fuel based on potential events.
- The FSAR approach results in no radiological release from the fuel, which has a number of effects on NRC findings throughout the review (security, environmental, SSC classification, etc.).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Conclusion

- Staff questions are related to the application of the MCA analysis approach as described in FSAR Sections 5.5 and 5.6. For potential events, a documented basis is required to ensure that the health and safety of the public and the environment is protected. Some examples of that basis could be that:
  - Consequences are low (demonstrated through analysis), for instance due either to a small source term or efficacy of engineered barriers
  - Consequences are bounded by an event that is previously analyzed (in the case of an MHA)

- More information is needed to evaluate event sequences discussed in the FSAR

- Note: this discussion does not account for security considerations, which may not involve the same hazards as operational hazards

- This meeting represents the first step in moving to address staff questions so that there is a clear path to making a safety finding