Oklo Responses to NRC Request for Additional Information 1: Aurora Step 1 – MCA

October 2020

Oklo Inc.

TABLE OF CONTENTS

1 RAI: AURORA STEP 1 – MCA - 1

Provide an explicit definition for "credible" as used by Oklo in the FSAR, including how it was used to screen or exclude events as "not applicable & not credible" in FSAR Section 5.4.

Provide the technical basis for why events considered for the MCA using the process described in FSAR Section 5.4 were limited to those involving a single failure, given the MCA is cited to meet all accident analysis requirements as well as provide a supporting basis for the proposed exemption from the requirement to assume a postulated fission product release (10 CFR 52.79(a)(1)(vi)). If this basis incorporates a frequency argument, provide a quantitative threshold for which events are excluded, and provide the technical basis behind the assumptions used to calculate the values used in assessing events against that threshold. If there are assumptions related to the functional capability or reliability of engineered safety features that are needed for an event to remain outside the scope of "credible," update the FSAR with the mechanism to capture these assumptions within the plant licensing basis.

1.1 Oklo response

The definition of "credible" as used by Oklo is described in Section 5.5.1 of the FSAR, which says that "[c]redibility is based on whether something is physically, fundamentally, or mechanistically possible." It is described more explicitly in the "Maximum Credible Accident Methodology: Summary of Methodology" document (referred to here as the "MCA methodology summary") uploaded to the electronic reading room as part of the MCA audit. The document presents two screening criteria that must be met for an event to be deemed "credible." In summary: the event must first be deemed phenomenologically applicable to the design (Criterion 1), it then must be deemed physically, fundamentally, or mechanistically possible (Criterion 2A), and it must be deemed to result from a single initiating event (Criterion 2B). If these criteria are met, the event is considered credible; otherwise, the event is screened out and not analyzed further.

Criterion 2B does not rule out events with multiple failures, but it requires a single initiating event be responsible for those failures. This means that event sequences with multiple failures, including common cause failures, can pass Criterion 2B and be deemed credible. This is described in Section 5.1.1 of the FSAR as well, which states that the methodology analyzes "any plausible single failure as well as any single initiating event to cause a common set of failures, even if extreme." As described in the MCA methodology summary, and Section 5.1.1 of the FSAR, in addition to the single initiating event that causes the MCA, an additional single failure is then assumed for defense-in-depth purposes.

The technical justification for the exemption to cybersecurity requirements, associated with 10 CFR 73.54, 10 CFR 73.77, and portions of 10 CFR 52.79(a)(36) and 10 CFR 73.55, does implicitly cite the MCA when it states: "In bounding accidents, the Aurora design cannot cause an offsite radiation dose to the public." However, the technical justification for the exemption rests primarily on two points:

- The simplicity of the reactor trip system, which does not rely on digital computers and communication networks that could be disrupted by cyber attack.
- The small inventory of radioactive fission products, which ensures that the reactor does not pose a risk to public health and safety.

The first point is the primary basis for the technical justification. The automatic reactor trip system is designed such that it is not vulnerable to cyber attack. Specifically, Part V of the COLA provides further information regarding the low-tech nature of the Aurora facility:

> …the automatic reactor trip system does not use "digital computer and communication systems and networks," as defined in 10 CFR 73.54(a). The automatic reactor trip system does not use any digital computers, does not use a communication system, and is not connected to a network. The reactor trip system limits can only be changed by physically accessing the trip system hardware which is located in an access controlled area of the Aurora facility.

The small inventory of the Aurora reactor additionally assures there is no appreciable risk to public health and safety. Therefore, neither of these justifications depend on the specific choice of MCA.

The technical justification for the exemption to licensed operators, associated with portions of 10 CFR 52.79(a)(14) and (34), as well as 10 CFR 50.54(i),(j),(k),(l),(m) and 10 CFR Part 55, explicitly refers to the MCA when describing the lack of credited operator actions (Part V, Section 3.5.1.2). However, as described above for the cyber security exemption, the technical justification for this does not depend on a specific choice of MCA. The primary justification for the exemption to licensed operators is the fully automated control system with no required operator actions. As stated in Part V Section 3.5.1.1:

> The only reactor control that is available to Onsite Monitors is the ability to initiate a reactor trip. While initiating a reactor trip does directly affect the reactivity and power level of the reactor, this action can only put the reactor into a shutdown state.

In addition to the fully automated controls, the small inventory of radioactive fission products ensures that the reactor does not pose a risk to the public health and safety. The specific case of the MCA was included in Part V as illustrative of the fact that no operator actions are required to achieve a safe state even in the case of the most challenging credible event identified, but the technical justification does not depend on the choice of a specific MCA. Part V of the COLA will be updated to clarify that the technical basis to this exemption lies in the automatic nature under which the Aurora is controlled.

The technical justification for the exemption to offsite emergency planning, associated with portions of 10 CFR 50.47 and 10 CFR Part 50, Appendix E, explicitly refers to the zero release from the MCA. However, the primary technical basis for this exemption is that there is no postulated accident that would exceed the proposed emergency planning dose criteria. This criteria is stated in the FSAR and is explicitly re-stated in Part V of the COLA, in the following way:

> As the basis in NRC emergency planning guidance is for the size of the EPZ to be based on the PAGs, an offsite emergency preparedness plan needs to exist if there is a possibility of an accident which would result in a 1 rem projected dose[1] to a member of the public.

[1] The NRC's policy statement incorporating NUREG-0396 was released October 23, 1979 in 44 FR 61123.

The small inventory of radioactive fission products ensures that the reactor does not pose a risk to public health and safety. There are no events that are postulated to exceed the above criteria. Part V will be updated to clarify this point.

The Issue portion of the RAI states that there is "no stated need to mitigate against the consequences of radiological releases" in Section 5.2 of the FSAR and asserts that Oklo's safety principles are incomplete. However, the relevant safety principle in Section 5.2.1 is as follows (emphasis added): "Restrict the likelihood **and consequence** of abnormal events by inherent, physical characteristics." The safety goal of the Aurora is to maintain fuel integrity because the fuel matrix is the first barrier to the release of fission products. The fuel material chosen therefore restricts both the likelihood and consequence of abnormal events by its inherent, physical characteristics, thus mitigating against consequences of radiological release and meeting both the safety principle above, and the intent of the IAEA safety principles.

1.2 Associated changes to the COLA

The following portions of the COLA will be revised as described above and shown in the provided markup below.

Part V, Section 3.5.1.2:

> Onsite Monitors do not perform any credited operator actions to ensure public health and safety. ~~the reactor maintains a safe state~~. ~~As shown in Chapter 5, "Transient analysis," of Part II, the maximum credible accident (MCA) assumes a complete loss of heat sink in conjunction with a failure to insert one of three shutdown rods.~~ When trip setpoints are exceeded, ~~two of three~~ shutdown rods are ~~assumed to be~~ automatically inserted, and the reactor is shut down. Following shutdown, decay heat is transferred away from the fuel ~~by entirely passive and inherent means,~~ primarily through the heat pipes to the working fluid of the power conversion system, and ultimately to the environment. Even in the event of a total loss of heat sink, decay heat is transferred by entirely passive and inherent means, primarily through conduction to nearby structures~~.~~ ~~Decay heat~~, and is ultimately removed by natural convection to the air in the reactor cavity. It is important to note that Onsite Monitors do not have any credited actions during any postulated events.

Part V, Section 3.6, page 34:

> ~~Due to the Aurora design having no credible radiological release,[4] the Aurora EPZ is limited to the Aurora powerhouse.~~ Since the Aurora powerhouse contains the EPZ, the parts of 10 CFR 50.47 and 10 CFR Part 50, Appendix E related to offsite emergency monitoring and response no longer serve the underlying the intent of the regulation to ensure rapid response to protect the public in the case of an offsite radiological event.

The footnote on the bottom of page 34 of Part V will also be deleted:

> ~~As shown in Chapter 5 of Part II, there are no credible accidents that result in the release of radioactive material; the MCA, which assumes a complete loss of the secondary system in conjunction with a failure to insert one of the shutdown rods, does not result in a radioactive release.~~

Part V, Section 3.6.1:

> For the Aurora, the plume exposure and ingestion exposure pathway comprise the same EPZ, which is limited to the exterior boundary of the Aurora powerhouse. Since the EPA PAGs are met by the Aurora, ~~As there is no radiological release associated with the MCA, the PAGs are met through an~~, the EPZ is limited to the Aurora powerhouse. ~~The MCA is discussed in Chapter 5 of Part II.~~

2 RAI: AURORA STEP 1 – MCA - 2

Demonstrate that a comprehensive review of the potential initiating events and various equipment failure modes have been considered and appropriately evaluated in the selection of the MCA. The evaluation should include effects on the reactor, potential releases from those events, and failures of equipment that would be considered non-safety related in order to ensure that all appropriate events are considered. The review should include all operating conditions including normal, abnormal, and accident scenarios during various plant operating modes such as start-up and shutdown conditions. If, after this review, an event different from the current licensing basis is determined to be the MCA, revise the FSAR accordingly. In addition, provide information which discusses the additional scenarios evaluated so that the NRC staff can understand and evaluate the full breadth and scope of events considered.

2.1 Oklo response

The methodology Oklo uses to select the MCA for its reactor designs is summarized in the "Maximum Credible Accident Methodology: Summary of Methodology" document uploaded to the electronic reading room as part of the MCA audit. Appendix B of that document describes the specific application of the more general MCA methodology to the Aurora design. In addition, the spreadsheet titled "Oklo MCA methodology – event down-selection for the Aurora," also uploaded to the electronic reading room, provides the full list of events considered in this application of the MCA methodology and details how each event was treated through each step of the methodology. These documents, along with Chapter 5 of the FSAR, describe the process that was used to select the MCA for the Aurora.

2.2 Associated changes to the COLA

There are no changes to the COLA as a result of this response at this time.

3 RAI: AURORA STEP 1 – MCA - 3

Identify if the MCA analysis assumes that the reactor cell can leaks. Provide the design basis for assumed reactor cell can leakage (including zero, if applicable) and document in the FSAR.

If the design basis for the MCA is that the reactor cell can may leak, provide an evaluation of MCA consequences based on the assumed leakage and update the FSAR accordingly.

3.1 Oklo response

3.1.1 Summary

Oklo recognizes the NRC staff's interest in the assumptions of the MCA analysis as it relates to leakage of the reactor cell can. The reactor cells are designed and fabricated to be leak tight to support continuity of normal operations. However, the MCA analysis does not assume reactor cell cans to be leak tight. Radionuclides, primarily fission products, are retained within the fuel matrix and are therefore not expected to be present in the gas plenum during normal operation. Further, because the fuel is not damaged during the MCA, there is no additional contribution of leakage of radionuclides during the MCA. The relevant characteristics of the fuel related to confinement of radionuclides are ensured through a design commitment with applicable programmatic controls. Design commitments are not made for the reactor cell cans to be leak tight because reactor cell cans are not assumed to be leak tight in the safety analysis. This is consistent with the approach used throughout the FSAR, and is explained in the context of the safety analysis in Section 5.6.2.1 of the FSAR.

3.1.2 Background

Relevant background information is provided in this section, primarily as described in FSAR.

The following excerpts are included from Section 4.2.1, "Principal Design Criteria 1: Confinement" of the FSAR:

> PDC 1 is unique to the Aurora, and is presented below:
>
> > Structures, systems, and components responsible for maintaining confinement of radionuclides for the Aurora will perform their required functions during off-nominal events up to and including the maximum credible accident, or will minimize the severity of the challenges to those functions.
>
> Specifically, since the fuel matrix is the primary confinement feature in the Aurora, the application of Appendix B quality assurance regarding fuel will ensure that the fuel is manufactured, shipped, stored, etc. in a quality assured manner in all stages.
>
> […]
>
> Metal fuel, like other metals, is a relatively nonporous solid with a regular crystal lattice. As a result, and as shown in extensive data from decades of operation, the vast majority of fission products are retained within the fuel matrix at burnups less than 1%.

PDC 1 is met through a design basis for the reactor core system, DB.RXS.01, and this design basis is ensured through design commitment DC.RXS.01.A, which is presented below:

Design basis:

DB.RXS.01 The reactor core system uses metal fuel with well characterized properties.

Design evaluation summary:

The analysis in this section has shown that the steady state operating temperature of the reactor core system provides substantial margin to fuel-steel eutectic formation temperatures at full power. The safety analysis in Chapter 5 shows that this margin is sufficient to maintain the safety and operational goals of the Aurora in the event of the maximum credible accident. A design commitment is taken to the ensure that the fuel used in the Aurora meets the critical characteristics required to maintain the safety and operational goals, and the appropriate programmatic controls are in place to ensure the commitments are met.

Design commitments and programmatic controls:

DC.RXS.01.A The fuel in the reactor system is procured according to 10 CFR Part 50 Appendix B, with a critical characteristic of thermal conductivity.

(see Oklo Quality Assurance Program Description)

As described in Section 5.3.1, "Safety goal: control release of radionuclides," of the FSAR, "[t]he safety limit is set such that the fuel temperature remains below the melting (solidus) temperature of 1200 C. Fuel melt is to be avoided in the Aurora because the fuel significantly loses its capability to retain fission products upon melting."

3.1.3 Detailed response

As described in Fast Reactor Working Group 18-01 white paper, "Nuclear Metal Fuel: Characteristics, Design, Manufacturing, Testing, and Operating History,"[2] at low burnups, because of the "gradual interconnection of fission gas bubbles, the release of fission gas to the plenum is not constant," and "[i]nitially, no fission gas is released, as it stays entirely contained in the bubbles" [1]. At approximately 1 atom percent (at. %), fission product generation is sufficient to enable interconnection of pores, and gaseous fission products are able to collect in the gas plenum.

Because of the low burnup of fuel in the Aurora (less than 1 at. %), during normal operation, this interconnection of pores is not expected to occur; thus, the only fission products that are able to collect in the gas plenum are fission products that are generated on the surface of the fuel and able to migrate through the sodium bond to the gas plenum. These surface-generated

[2] ML18165A249

fission products are a small contribution to the total generation of fission products and are therefore neglected. It is important to note that the total fission product inventory in the Aurora core after 20 years is less than 0.5% of the inventory generated in a 3,000 MWth pressurized water reactor (PWR) core halfway through one cycle.

While burnup and interconnection of pores are the main drivers of fission product generation in the plenum, fission products may be released from the fuel matrix at a significantly higher rate in the event of fuel melting. Because fuel temperatures during the MCA are significantly below the fuel melting (solidus) temperature of 1200C, the MCA does not result in damage to the fuel, and this additional contribution does not occur.

Therefore, due to the retention of fission products within the fuel matrix, the reactor cell cans need not be leak tight, and a design basis is not taken for their leak rate. In other words, the reactor cells are not assumed to be leak tight for the safety analysis, and therefore require no design basis on this feature. Similarly, the additional barriers to fission product release between the fuel matrix and the environment (e.g., the capsule and the module shell) are designed and fabricated to be leak tight, but they are not relied on or assumed to be leak tight in the safety analysis. In practice, all of these barriers would have very low leak rates, but the barriers are not necessary to ensure the confinement of radionuclides because this is accomplished by the fuel matrix and ensured by the relevant programmatic controls on the fuel.

While beyond the scope of this request, Oklo notes that the Aurora powerhouse is equipped with continuous air monitors, allowing continuous radiation monitoring in the building basement, and readings are displayed in the monitoring room. These radiation monitors are described in Section 6.2 of the "Radiation Protection Program," Enclosure 4, to the Aurora COLA:

> The air in the building basement is constantly monitored with continuous air monitors. Radiation monitoring in the building basement is performed with remote instrumentation, with readings displayed in the monitoring room.

3.2 Associated changes to the COLA

There are no changes to the COLA as a result of this response at this time.

4 RAI: AURORA STEP 1 – MCA - 4

Update the FSAR to incorporate one of the following to support the MCA evaluation presented in FSAR Section 5.5:

1. Provide the analysis, appropriate test programs, experience, or a combination thereof to support the efficacy of the measurement technique described in FSAR Section 2.7.2.7.2, especially as it relates to the statement "fuel temperatures can be inferred from heat pipe temperatures" and demonstrate that a reactor trip initiated through the measurement technique described in FSAR Section 2.7.2.7.2 is sufficiently reliable such that unprotected LOHS or unprotected heat pipe degradation/failure events do not need to be considered as candidates for the MCA.

OR

2. Provide evidence of diversity in the instrumentation and control system (i.e., the ability to initiate automatic reactor trip signals based on measurement techniques diverse from the method described in FSAR Section 2.7.2.7.2) to show that the measurement technique described in FSAR Section 2.7.2.7.2 is not the only means to detect adverse conditions, and demonstrate that the credited instrumentation is sufficiently reliable such that unprotected LOHS or unprotected heat pipe degradation/failure events do not need to be considered as candidates for the MCA.

OR

3. Evaluate the unprotected LOHS and unprotected heat pipe degradation/failure events to ensure all appropriate events are included in the MCA.

4.1 Oklo response

4.1.1 Summary

Oklo recognizes the NRC staff's interest in the measurement techniques described in the FSAR, specifically as it relates to the consideration of unprotected events. Of the three response methods described in the RAI request, Oklo takes the first approach and interprets this to contain two components, discretized as (1) "Provide the analysis, appropriate test programs, experience, or a combination thereof to support the efficacy of the measurement technique…" and (2) "demonstrate that a reactor trip initiated through the measurement technique […] is sufficiently reliable" to screen out unprotected events.

As such, this response is discretized to respond to each of these components. The first component is provided through a combination of experience and test programs and is ultimately ensured through a design commitment and programmatic controls to conduct testing prior to operation. The second component is provided through a description of the system response to each event sequence described, with a focus on the redundancy of credited detection capabilities and the reliability of the reactor trip system following detection, with supplemental description of diverse measurement techniques. Ultimately, per Oklo's MCA methodology, unprotected loss of heat sink (LOHS) and unprotected heat pipe degradation or failure event sequences are not considered as candidates for the MCA.

4.1.2 Detailed response

4.1.2.1 Efficacy of measurement technique

Oklo recognizes that the measurement technique of thermocouples in the condenser region of a heat pipe to infer fuel temperature is an innovative approach for commercial fission systems. However, the usage of thermocouples in the condenser region of heat pipes is common practice when measuring heat pipe performance [2][3]. As shown in the KRUSTY experiment, the usage of thermocouples in the condenser region of heat pipes in heat pipe cooled fission systems has demonstrated successful detection of off-normal behavior in response to startup, loss of heat sink, and reactivity insertion events [3].

In response to reactivity insertion events, the experiment showed that the "response time between the reactivity insertion, the core temperature, and the heat pipe vapor temperatures is indistinguishable" and that the heat pipe vapor "responds to changes in the core temperature and is able to transfer the heat very quickly to the condenser" [3]. Further, in response to loss of heat sink (Stirling engine shutoff) events, thermocouples in the condenser region of the heat pipes indicated a faster and higher magnitude response than thermocouples adjacent to the reactor core, and core and heat pipe vapor temperatures were shown to be in phase with each other after the initial thermal lag between the convertor and core [3].

While this operating experience and understanding of the Aurora system provides confidence in the measurement technique, Oklo recognizes the importance of this measurement technique to the operation of the reactor trip system, and proposes the addition of a design commitment DC.ICS.01.E and associated programmatic controls to design basis DB.ICS.01 to ensure the efficacy of the measurement technique. The FSAR will be updated to reflect this addition.

4.1.2.2 Reliability of reactor trip

The reactor trip system, described in Section 4.1.2.2.1, is designed to reliably detect and respond to conditions necessitating reactor trip. Operational redundancy is provided by the plant control system, as described in Section 4.1.2.2.2. The initiating events discussed in this RAI, namely heat pipe degradation or failure and loss of heat sink, result in a system response that is detectable within seconds of the initiating event by both the reactor trip system and the plant control system. Sections 4.1.2.2.3 and 4.1.2.2.4 describe the response of the reactor trip system to these initiating events, as well as the diversity and redundancy of sensors that are able to detect the off-normal conditions as part of the plant control system.

4.1.2.2.1 Reactor trip system

As described in Section 2.7.1 of the FSAR, the reactor trip system is the "only subsystem [of the instrumentation and control system] credited in the safety analysis in Chapter 5, and therefore contains the only design bases for the instrumentation and control system." The reactor trip system utilizes well characterized, reliable, and redundant components, which results in highly reliable system behavior. The reliability and effectiveness of the reactor trip system is ultimately ensured by six design bases, with a total of sixteen design commitments (after the proposed addition described in this RAI response), each with the appropriate pre-operational tests (POTs), startup tests (SUTs), and technical specifications (TS) to ensure that the system operates as designed.

These programmatic controls are fundamental to the Aurora COLA and ensuring that this first-of-a-kind technology will be operated within its design limits. The programmatic controls are performance-based and represent the "appropriate test programs" that will be used to verify the

efficacy of the reactor trip system, including the measurement technique that is the subject of this RAI. They are explicitly committed to as license conditions that must be completed prior to startup (POTs must be completed to satisfy an ITAAC), as tests that must be completed during startup (SUTs) and as the operating limits of the reactor (TS) that ensure they continue to be effective during normal operation.

Of the design bases for the reactor trip system, design basis DB.ICS.01 and its associated design commitments and programmatic controls, is particularly relevant to detecting the events discussed in this RAI response:

Design basis:

DB.ICS.01 The reactor trip system monitors reactor process variables and sends a reactor trip signal when a process variable exceeds a limit setpoint.

Design evaluation summary:

This section describes the design of the reactor trip system, which provides the ability to detect and respond to multiple trip conditions. The transient analysis in Chapter 5 shows that if reactor trip signals are sent in response to the chosen setpoints, and the shutdown rods insert within the appropriate time interval, then fuel temperatures will be maintained below the required limits. Design commitments are made to ensure that each of the trip conditions will be reliably detected, and will result in a reactor trip signal, and the appropriate programmatic controls are in place to verify it.

Design commitments and programmatic controls:

DC.ICS.01.A The reactor trip system sensors are installed in the correct locations.

POT.ICS.01.A1 and A2 (see Chapter 14)

SUT.ICS.01.A1

DC.ICS.01.B The reactor trip system process limit monitors are connected to the correct locations, and are configured with the correct sensor scaling information and limit setpoints.

POT.ICS.01.B1 and B2

TS.LCO.02 (see Part IV)

DC.ICS.01.C The reactor trip system sensors are connected to the correct process limit monitors.

POT.ICS.01.C1 and C2

SUT.ICS.01.C

DC.ICS.01.D The reactor trip system process limit monitors send a fault signal when a process variable exceeds a limit.

POT.ICS.01.D

TS.LCO.02

Process variables are monitored by sensors inside and outside the reactor module. Operating limits for process variables are defined to protect the reactor and equipment. Each operating limit is enforced by a limit monitor or sensor that sends a fault signal to the control logic when the process variable exceeds the defined operating limits.

Three functionally identical instrumentation enclosures provide redundancy. The analog signals from the redundant sensors are routed to one of the three instrumentation enclosures. The instrumentation enclosures include signal conditioning and process variable limit monitors.

Two functionally identical and independent control enclosures are included for redundancy, and the two control enclosures independently aggregate the independent fault signals to generate a reactor trip signal from each control enclosure. The two reactor trip signals are combined such that if either control enclosure signals a shutdown, a reactor shutdown occurs.

It is important to note that the two bounding analyses described in this document each assume that one of three shutdown rods fails to insert. Only one shutdown rod is needed to shut down the reactor, which is a design basis of the shutdown rod system (DB.SRS.01).

Of particular relevance to the events described in this RAI response is the aggregation of the heat pipe temperature fault signals, described by Section 2.7.3.4.2.1 of the FSAR. Thermocouples that have failed as an open-circuit or have been disconnected from the process limit monitor are automatically detected and reported with a fault signal to the aggregation logic. The aggregation of these fault signals enforces upper and lower temperature limits, and ensures that a reactor trip is initiated when over-temperature, under-temperature, or insufficient thermocouple conditions are detected.

Section 2.7.3.4.2.1 of the FSAR describes two criteria that must be met for each reactor cell heat pipe to prevent the initiation of a reactor trip by the reactor trip system. The second of these two criteria, which allows for the use of indirect temperature measurements to compensate for a lack of multiple direct temperature measurements, will be removed from the FSAR and will no longer be used by the reactor trip system.

4.1.2.2.2 Plant control system

In addition to the reactor trip system, the plant control system "performs plant-wide process monitoring and control, including plant automation and alarm indication" and "monitors heat pipe thermocouple data, reactor power data, and reactor period data." As described in Section 2.7.3.3 of the FSAR, the reactor trip system "can receive a trip signal from the plant control system" to provided defense-in-depth to the reactor trips initiated by the reactor trip system.

Two types of reactor trips implemented by the plant control system are explicitly mentioned in the FSAR, namely secondary loop trips and shutdown rod insertion time trips. Secondary loop trips are "initiated by pressure switches and thermocouples in the secondary loop, and by the power conversion system" and are for "defense-in-depth and investment protection purposes because the reactor trip system would already initiate a reactor trip on over-temperature" in the case of a loss of heat sink.

Although the reactor trip system will no longer utilize indirect temperature measurements in the aggregation of heat pipe temperature fault signals, as described in the section above, the plant control system will have the capability to monitor core-wide temperatures and infer the existence of local failures based on an aggregation of every thermocouple measurement. The plant control system cannot override the reactor trip system, and can only send additional trip signals, providing defense-in-depth.

4.1.2.2.3 Heat pipe failure

While many possible initiating events related to heat pipe performance were considered, a single heat pipe failure from a manufacturing defect with failure to insert one shutdown rod is the bounding event for the decrease in heat removal by the heat pipes (i.e., loss of cooling) event category. As such, Oklo's modeling of heat pipe performance in its bounding analysis is binary: operational or failed. Operational heat pipes are modeled with a high equivalent thermal conductivity, and failed heat pipes are modeled with a low thermal conductivity. Heat pipe failure results in an inability to effectively transfer heat from the fuel to the heat exchanger system; while the working fluid of the power conversion system (i.e., sCO_2) continues to circulate through the heat exchanger, heat is transferred to the sCO_2, resulting in a rapid temperature decrease in the heat exchanger region.

As shown in "Oklo Inc. – Heat pipe failure in the Aurora, Rev. 0," uploaded to the electronic reading room during the acceptance review audit, a heat pipe failure results in a rapid temperature decrease in the heat exchanger region; in this analysis, the credited under-temperature condition is met, a 10-second delay between trip setpoint and reactor trip is assumed to occur, and the reactor is then modeled in a tripped condition. The reactor cell that experiences a heat pipe failure has three thermocouples, resulting in three independent sensors that are able to detect an under-temperature condition.

While this direct under-temperature condition is credited in the system response to a heat pipe failure event, it is important to note that off-normal (over-temperature) signals in surrounding reactor cells are detectable by the thermocouples of these surrounding reactor cells, as well as off-normal signals in the power conversion system. These are not credited reactor trip conditions; however, it is important to note that diverse and redundant measurement techniques are available to detect off-normal system behavior through the plant control system.

4.1.2.2.4 Loss of heat sink

Similarly, while many initiating events may result in a partial loss of heat sink, the total loss of heat sink with a failure to insert one shutdown rod is the bounding analysis for the decrease in heat removal by the secondary system event category. The total loss of heat sink results in temperature increases throughout the reactor module, including in each of the 114 reactor cells, each of which has 3 thermocouples, resulting in 342 independent sensors that are able to detect an over-temperature condition.

While this direct over-temperature condition is credited in the system response to a loss of heat sink event, it is important to note that signals in the power conversion system would likely indicate off-normal system behavior faster than the over-temperature trip condition credited in Chapter 5 of the FSAR. These signals are highly dependent on the initiating event. While a total loss of heat sink is not considered a credible event sequence, the following off-normal system conditions are provided as examples of signals that may be detected through the plant control system to provide defense-in-depth through diverse and redundant measurement techniques for partial loss of heat sink event sequences:

- Inadvertent pump trip results in a decrease in sCO_2 pressure and flow rate at the inlet of the heat exchanger system
- Ultimate heat sink malfunction (air-cooled cooler or radiator) results in an increase in sCO_2 temperature at the outlet of the heat sink and inlet to pump

4.2 Associated changes to the COLA

The following portions of the COLA will be revised as described above, and shown in the provided markup below.

Part II, Sections 2.7.3.7 and 5.6.2.10:

Design basis:

DB.ICS.01 The reactor trip system monitors reactor process variables and sends a reactor trip signal when a process variable exceeds a limit setpoint.

Design evaluation summary:

This section describes the design of the reactor trip system, which provides the ability to detect and respond to multiple trip conditions. The transient analysis in Chapter 5 shows that if reactor trip signals are sent in response to the chosen setpoints, and the shutdown rods insert within the appropriate time interval, then fuel temperatures will be maintained below the required limits. Design commitments are made to ensure that each of the trip conditions will be reliably detected, and will result in a reactor trip signal, and the appropriate programmatic controls are in place to verify it.

Design commitments and programmatic controls:

DC.ICS.01.A The reactor trip system sensors are installed in the correct locations.

POT.ICS.01.A1 and A2 (see Chapter 14)

SUT.ICS.01.A1

[…]

DC.ICS.01.E The reactor trip system correctly infers fuel temperature based on heat pipe temperature.

POT.ICS.01.E1

POT.ICS.01.E2

POT.ICS.01.E3

Part II, Section 4.2.2:

Table 4-3: Design bases, commitments, and programmatic controls associated with PDC 2

Instrumentation and control system		
DB.ICS.01	The reactor trip system monitors reactor process variables and sends a reactor trip signal when a process variable exceeds a limit setpoint.	DC.ICS.01.A POT.ICS.01.A1 POT.ICS.01.A2 SUT.ICS.01.A1 DC.ICS.01.B POT.ICS.01.B1 POT.ICS.01.B2 DC.ICS.01.C POT.ICS.01.C1 POT.ICS.01.C2 SUT.ICS.01.C DC.ICS.01.D POT.ICS.01.D TS.LCO.02 DC.ICS.01.E POT.ICS.01.E1 POT.ICS.01.E2 POT.ICS.01.E3

Part II, Section 14.9:

Table 14-7: List of instrumentation and control system preoperational tests and objectives

Test identifier	Design basis	Objective
POT.ICS.01.A1	DB.ICS.01	Verify each flux detector is installed in the correct location in the reactor core.
POT.ICS.01.A2	DB.ICS.01	Verify each control drum absolute position sensor is installed in the correct location.
POT.ICS.01.B1	DB.ICS.01	Verify each process limit monitor is connected in the correct location in the junction box.
POT.ICS.01.B2	DB.ICS.01	Verify the process limit monitors are configured with the correct scaling information and limit setpoints.
POT.ICS.01.C1	DB.ICS.01	Verify each flux detector is connected in the correct location in the junction box.
POT.ICS.01.C2	DB.ICS.01	Verify each control drum absolute position sensor is connected in the correct location in the junction box.
POT.ICS.01.D	DB.ICS.01	Verify that each reactor trip system process limit monitor sends a fault signal when the measured value exceeds a limit.
POT.ICS.01.E1	DB.ICS.01	Verify that the output of a thermocouple in the condenser region of a heat pipe is directly correlated to the fuel temperature.
POT.ICS.01.E2	DB.ICS.01	Verify that the output of a thermocouple in the condenser region of a heat pipe decreases below the under-temperature limit setpoint following failure of the heat pipe.
POT.ICS.01.E3	DB.ICS.01	Verify that the output of a thermocouple in the condenser region of a heat pipe increases above the over-temperature limit setpoint following the loss of heat sink.
POT.ICS.02.A	DB.ICS.02	Verify the time between the exceedance of a limit setpoint and the reactor trip signal is less than the specified time.
POT.ICS.03.A	DB.ICS.03	Verify the functionality of each of the manual reactor trip buttons installed in the facility.
[…]	[…]	[…]

Part II, Section 14.9.1:

Frequency	The tests identified as FOAK are performed once for the Aurora design. ~~These~~ Other tests are required to be performed once per reactor.
Purpose	Completion of the following tests verifies that the tested components are installed correctly.
Prerequisites	Installation of each component must be completed prior to inspecting or testing the component.

…

Test identifier	**POT.BAS.02.B**
objective	Verify that openings and penetrations through fire barriers are protected according to design documents referenced by the test procedure.
method	Visual inspection and measurements of the components installed to protect fire barrier openings and penetrations, and comparison to referenced design documents.
acceptance criteria	Openings and penetrations through fire barriers are protected by components (e.g. fire doors, fire dampers, or penetration seals) having fire resistance equivalent to those of the barrier.
Test identifier	**POT.ICS.05.C**
objective	Verify the control cabinets and instrumentation cabinets are installed in an access-controlled area.
method	Confirmation that access-control features are in place to protect the control and instrumentation cabinets from unauthorized access.
acceptance criteria	The process limit monitors are installed in an access-controlled area to prevent changes to limit setpoints, scaling information, or other configuration by unauthorized personnel.
Test identifier	**POT.ICS.01.E1 (FOAK)**
Objective	Verify that the output of a thermocouple in the condenser region of a heat pipe is directly correlated to the fuel temperature.
method	Instrument a prototypic reactor cell with thermocouples in the condenser region of the heat pipe and in the surrogate fuel material. Apply varying thermal loads to the surrogate fuel material through non-nuclear heating.
acceptance criteria	The measured temperatures in the surrogate fuel material and the condenser region of the heat pipe sufficiently match the predicted correlation.
Test identifier	**POT.ICS.01.E2 (FOAK)**
Objective	Verify that the output of a thermocouple in the condenser region of a heat pipe decreases below the under-temperature limit setpoint following failure of the heat pipe.
method	Instrument a prototypic reactor cell with thermocouples in the condenser region of the heat pipe and in the surrogate fuel material. Apply the nominal thermal load at full power to the surrogate fuel material through non-nuclear heating. Initiate a heat pipe failure.
acceptance criteria	The measured temperature response in the surrogate fuel material and the condenser region of the heat pipe sufficiently match the predicted response.
Test identifier	**POT.ICS.01.E3 (FOAK)**
Objective	Verify that the output of a thermocouple in the condenser region of a heat pipe increases above the over-temperature limit setpoint following the loss of heat sink.
method	Instrument a prototypic reactor cell with thermocouples in the condenser region of the heat pipe and in the surrogate fuel material. Apply the nominal thermal load at full power to the surrogate fuel material through non-nuclear heating. Initiate a loss of heat sink.
acceptance criteria	The measured temperature response in the surrogate fuel material and the condenser region of the heat pipe sufficiently match the predicted response.

Part II, Section 2.7.3.4.2.1:

> The fault signals are aggregated such that ~~at least one of~~ the following criterion~~a~~ must be met for each reactor cell heat pipe: ~~(1)~~ two or more direct temperature channels shall not be sending a fault signal (schematic shown in Figure 2-25)~~, 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~~. If any of the reactor cell heat pipe temperature channels do not meet thi~~s~~ese criterion~~a~~, the reactor trip system automatically initiates a reactor trip within 5 seconds.

5 REFERENCES

[1] Fast Reactor Working Group, "Nuclear Metal Fuel: Characteristics, Design, Manufacturing, Testing, and Operating History," ML18165A249, Jun. 2018. [Online]. Available: https://oklo.box.com/s/82c1895czzgw2vgf474wcxmuk6ut4qx0.

[2] A. J. Clark, "Failures and Implications of Heat Pipe Systems," Sandia National Laboratories, Albuquerque, NM, SAND2019-11808, 2019.

[3] M. A. Gibson, D. I. Poston, P. McClure, and J. L. Sanzi, "Heat Transport and Power Conversion of the Kilopower Reactor Test," *Nuclear Technology*, vol. 206, pp. 31–42, 2020.