Part IV: Technical Specifications

TABLE OF CONTENTS

1 Introduction ... 3
1.0 Purpose ... 3
1.1 Format ... 3
1.2 Definitions ... 3
2 Safety limit ... 6
2.1 Safety limit ... 6
2.2 Safety limits violations ... 6
3 Limiting conditions for operation and surveillance requirements ... 7
3.1 Shutdown rod system ... 7
3.2 Reactor trip system ... 8
4 Design features ... 9
4.1 Reactor system ... 9
4.2 Control drum system ... 9
4.3 Shutdown rod system ... 9
4.4 Building system ... 9
5 Administrative controls ... 10
5.1 Organization ... 10
5.1.1 Structure ... 10
5.1.2 Responsibilities ... 10
5.1.3 Staff training ... 10
5.2 Procedures ... 11
5.3 Reportable events and required actions ... 11
5.3.1 Safety limit violation ... 11
5.3.2 Failure to meet limiting conditions for operation ... 12
Appendix A: Technical Specifications bases ... 13
A.1 Safety limit bases ... 13
A.2 Limiting conditions for operation and surveillance requirement bases ... 14
A.2.1 Shutdown rod system – LCO.01 basis ... 14
A.2.2. Reactor trip system – LCO.02 basis ... 15
A.3 Design feature bases ... 17
A.3.1 Reactor system ... 17
A.3.2 Control drum system ... 18
A.3.3 Shutdown rod system ... 19
A.3.4 Reactor module placement ... 19
A.4 References ... 19

1 INTRODUCTION

1.0 Purpose

Title 10 of the *Code of Federal Regulations* (10 CFR) Section 52.79(a)(30) requires the following, "Proposed technical specifications prepared in accordance with the requirements of §§ 50.36 and 50.36a of this chapter."

The purpose of this part is to address the requirements of 10 CFR 50.36, "Technical specifications," by providing the Technical Specifications (TS) for the Aurora located at the Idaho National Laboratory Site. The appendix to this document, "Technical Specification bases," provides the reasons for the TS. The TS bases are included as required by 10 CFR 50.36(a)(1) but are not part of the TS and do not constitute limitations or requirements to which Oklo Power must adhere.

1.1 Format

The TS are derived from analyses included in Part II, "Final safety analysis report." The format of the TS is informed by ANSI/ANS-15.1-2007, "The development of technical specifications for research reactors," since the Aurora is approximately the same size as a research reactor. Standard technical specifications (STS) for light water reactors (LWRs) were reviewed in the creation of these TS. However, the Aurora design intentionally minimizes human interaction with the plant and does not include many of the systems described by the LWR STS.

The TS are composed of a safety limit (SL), limiting conditions for operation (LCO), surveillance requirements, design features, and administrative controls. All of the LCOs use the following abbreviations:

- Applicability (APP)
- Condition (COND)
- Required action (REQ)
- Time (TIME)
- Surveillance requirement (SR)

Applicability (APP) describes when the LCO applies. Conditions (COND) describe the way an LCO is not met; conditions may be entered independently, as noted in the LCO. Required actions (REQ) define the actions needed to exit a condition (COND) and meet the associated LCO. Time (TIME) specifies the maximum amount of time for the required action (REQ) to be completed. Surveillance requirements (SR) are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the LCO will be met.

1.2 Definitions

The following terms are used throughout the TS.

applicability (APP): In the context of limiting conditions for operation (LCO), applicability describes the reactor states to which the LCO applies.

automatic reactor trip: The initiation of a reactor shutdown by an automated control action. An automatic reactor trip does not require any user action to initiate, and an automatic reactor trip cannot be prevented by user action.

biennial interval: In the context of surveillance requirements, a 2 year interval, not to exceed 2.5 years without a written directive signed by the Director of Reactor Operations. This directive shall be placed in the records and should indicate the reason for postponement and the expected completion date of the surveillance requirement.

channel: A channel is the combination of components including a sensor, lines, amplifiers, output devices, and a limit monitor that are connected for the purpose of measuring the value of a parameter and enforcing operational limits.

cold shutdown: State when the reactor temperature is near ambient temperature and the reactor is subcritical. Maintenance activities requiring disassembly of the reactor enclosures are performed in this state.

condition (COND): In the context of an LCO, a condition is the way that an LCO is not met.

design feature (DF): Design features are those features of the facility such as materials of construction and geometric arrangements, which, if altered or modified, could have an impact on safety and are not covered under limiting conditions for operation.

hot standby: State when the reactor temperature is decreasing to ambient and the reactor is subcritical.

limiting conditions for operation (LCO): Limiting conditions for operation are the lowest functional capability or performance levels of equipment required for safe operation of the facility.

power operation: State when the reactor is at operating temperature, the reactor power is generally at steady-state but may be increased or decreased, and significant power is being produced.

process limit monitor: A device that measures an analog signal from a sensor, compares the measured value to one or more limit setpoints, and sets the state of one or more digital outputs based on the result of the comparison(s).

reactor shutdown: A reactor shutdown is achieved if the reactor is subcritical and at least one shutdown rod is fully inserted into the core.

reactor trip: The initiation of a reactor shutdown by an automated control action or by a user action that results in the rapid insertion of the shutdown rods into the core and the core becoming subcritical.

reactor trip circuit: A hard-wired fail-safe circuit that aggregates fault signals and trip signals and determines whether or not the shutdown rod electromagnets should be de-energized to shut down the reactor.

required action (REQ): In the context of an LCO, required actions define the actions needed to restore the capability or performance level of equipment in order to exit a condition (COND) and meet the associated LCO.

rod insertion time: The elapsed time between the initiation of a reactor trip and the instant the shutdown rod reaches its fully inserted position. Rods are inserted into the core by gravity.

safety limit (SL): A limit on an important process variable that are found to be necessary to reasonably protect the integrity of certain physical barriers that guard against the uncontrolled release of radioactivity. Safety limits do not have to be measured directly; they may be derived from important process variables.

shall, should, may: The word "shall" is used to denote a requirement; the word "should" is used to denote a recommendation; and the word "may" is used to denote permission, neither a requirement nor a recommendation.

shutdown rod: A reactivity control device fabricated from a neutron-absorbing material that is inserted into the core to make the reactor subcritical. During power operation, a shutdown rod is suspended above the core by an electromagnet and is inserted into the core by gravity when the electromagnet is de-energized.

specifications: Specific limitations and equipment requirements for safe reactor operation and for dealing with abnormal events. Specifications are imposed as safety limits, limiting conditions for operation, surveillance requirements, and design features.

startup: State when the reactor temperature is being increased, and the reactor power is being increased, but the reactor is not producing significant power.

surveillance requirement (SR): Surveillance requirements are requirements relating to test, calibration, or inspection to assure that the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met. Surveillance requirements may be based on periodic intervals or may be triggered by other events or conditions.

time (TIME): In the context of an LCO, time specifies the maximum amount of time for the required action (REQ) to be completed.

2 SAFETY LIMIT

2.1 Safety limit

The following safety limit (SL) shall not be exceeded during power operation:

SL.1 The fuel temperature shall be maintained < 1,200 C.

2.2 Safety limits violations

If **SL.1** is violated, restore compliance and be in hot standby within 1 hour.

3 LIMITING CONDITIONS FOR OPERATION AND SURVEILLANCE REQUIREMENTS

3.1 Shutdown rod system

LCO.01 All shutdown rods shall fully insert into the core within 4 seconds of receiving a reactor trip signal.

APP.01. These specifications shall apply during startup and power operation.

Note: Independent condition entry allowed.

COND.A One shutdown rod does not fully insert within 4 seconds of receiving a reactor trip signal.

REQ.A.1 Restore the shutdown rod system to meet LCO.01 and perform SR.01.01.

TIME.A.1 90 days. (If REQ.A.1 is not met, a reactor trip is automatically initiated.)

COND.B Shutdown rod insertion time outside of required time resulted in an automatic trip.

REQ.B.1 Restore the shutdown rod system to meet LCO.01.

TIME.B.1 Prior to routine power operation.

SR.01.01 Following any activity that includes removal of the module equipment housing, LCO.01 shall be functionally tested in cold shutdown prior to functional testing starting from power operation. Following modifications or repairs to address the shutdown rod insertion time that do not include removal of the module equipment housing, LCO.01 shall be functionally tested starting from power operation.

SR.01.02 LCO.01 shall be functionally tested starting from power operation on a biennial interval. The reactor shall not return to routine power operation until such time that all surveillances are current and up to date.

SR.01.03 Reactor trips that satisfy LCO.01 and the surveillance requirements in SR.01.02 may be used to reset the surveillance interval before the next required surveillance for LCO.01.

3.2 Reactor trip system

LCO.02 The reactor trip system shall be functional.
APP.02. These specifications shall apply to the reactor during startup and power operation.

Note: Independent condition entry allowed.

COND.A One reactor trip circuit is not functional because the reactor trip circuit bypass switch is enabled.
REQ.A.1 Restore the reactor trip system to meet LCO.02.
TIME.A.1 7 days. (If REQ.A.1 is not met, a reactor trip is automatically initiated.)
COND.B Reactor trip system component caused an automatic reactor trip or is preventing reactor startup.
REQ.B.1 Restore the reactor trip system to meet LCO.02.
TIME.B.1 Prior to startup.

SR.02.01 The functionality of both reactor trip circuits shall be tested after any significant modifications, changes, or repairs to the reactor trip circuits and on a biennial interval. The reactor shall not return to power operation until such time that all surveillances are current and up to date.

SR.02.02 Each reactor trip system channel shall be functionally tested after any significant modifications, changes, or repairs to the reactor trip system process limit monitors or associated channel and on a biennial interval. The reactor shall not return to power operation until such time that all surveillances are current and up to date.

SR.02.03 Each manual reactor trip button in the facility shall be functionally tested after any significant modifications, changes, or repairs to the reactor trip circuits or a manual reactor trip button and on a biennial interval. The reactor shall not return to power operation until such time that all surveillances are current and up to date.

SR.02.04 Reactor thermal power channels shall be calibrated both (1) after any significant modifications, changes, or repairs to a reactor thermal power channel, and (2) according to instrumentation manufacturer's recommendations or a biennial interval. The reactor shall not return to power operation until such time that all surveillances are current and up to date.

4 DESIGN FEATURES

4.1 Reactor system

DF.01.01 The core shall consist of { }reactor cells, arranged in a hexagonal lattice in { }rings. All special nuclear material is low enriched and is contained in the reactor cells. {

}

DF.01.02 The { } absorber cells remain as configured during the Initial Test Program. This configuration is used to adjust the initial reactivity of the core, ensuring the core has the correct excess reactivity. Further adjustment would be considered a significant core configuration change.

DF.01.03 The systems surrounding the reactor core shall have the correct geometry, materials, and arrangement to conduct heat from the active core region to the module shell.

4.2 Control drum system

DF.02.01 The control drum system shall have a total reactivity worth of less than 700 pcm at all operating conditions.

DF.02.02 The control drum system shall be limited to rotation speeds of less than 1×10^{-2} deg/sec.

DF.02.03 The control drums shall be rotated using stepper motors.

4.3 Shutdown rod system

DF.03.01 The reactor shall include three shutdown rods that are held in place by electromagnets.

DF.03.02 Each shutdown rod shall have a minimum reactivity worth of 1,400 pcm.

4.4 Building system

DF.04.01 The reactor shall be housed in the basement of the Aurora powerhouse. The reactor module shall be located in the reactor module emplacement and have a cavity between the reactor module and the reactor module emplacement.

DF.04.02 The basement contains the reactor module, which is the only area in the facility that houses special nuclear material (SNM). The SNM is used at the Aurora facility by being irradiated in the reactor. Temporary storage of fuel is governed by the appropriate maintenance procedures.

5 ADMINISTRATIVE CONTROLS

5.1 Organization

5.1.1 Structure

The Aurora shall be owned and operated by Oklo Power, LLC (Oklo Power). The line management for Oklo Power, shown in Figure 1, shall provide for personnel who will administer and monitor the facility. The organization shall be responsible for safeguarding the public and onsite personnel and for adhering to all requirements of the license.

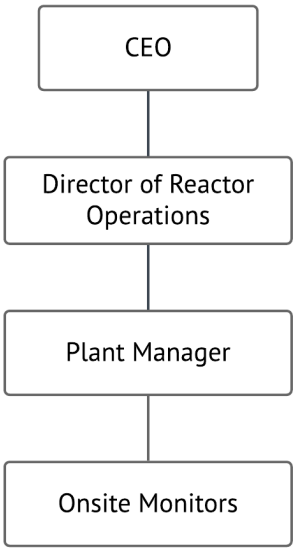

Figure 1: The line management for Oklo Power

5.1.2 Responsibilities

The responsibility of the safe operation of the Aurora is in accordance with the line management. The line management is the following:

- The Chief Executive Officer (CEO) shall be responsible for the Aurora license.
- The Director of Reactor Operations shall be responsible for reactor operation, adherence to the regulations, facility license, TS, and shall report to the CEO.
- The Plant Manager shall be responsible for the day-to-day reactor operation, including shift operation, and shall report to the Director of Reactor Operations.

5.1.3 Staff training

The selection and training of plant personnel shall be in accordance with the following:

- Responsibility: The Director of Reactor Operations shall be responsible for the selection and training of the Plant Manager and Onsite Monitors.

- Selection: The selection of Plant Manager and Onsite Monitors shall be consistent with the qualification requirements of the Oklo Power Training Program.

- Training: Plant Manager and Onsite Monitors shall complete the Oklo Power Training Program prior to duty.

5.2 Procedures

Written procedures shall be established, implemented and maintained covering the following activities:

- Maintenance

- Surveillance requirements, calibration and testing required by the TS

- Changes to the TS bases

Changes to procedures shall be made effective only after documented review by the Plant Manager and Director of Reactor Operations. Temporary deviations from the procedures may be made by the Onsite Monitors in order to address special or unusual circumstances or conditions; such deviations shall be documented and reported within 24 hours or the next working day to the Plant Manager.

5.3 Reportable events and required actions

5.3.1 Safety limit violation

In the event of a safety limit violation, the following actions shall be taken:

1. The reactor shall be shut down and reactor operation shall not be resumed until authorized by the U.S. Nuclear Regulatory Commission (NRC) pursuant to 10 CFR 50.36(c)(1).

2. The safety limit violation shall be reported to the NRC as soon as practical and within 4 hours of occurrence in all cases, in accordance with 10 CFR 50.72.

3. A review of the event shall be conducted, and the results of the review shall be recorded, including the cause of the condition and the basis for corrective action taken to prevent recurrence.

4. A record of the results of the review shall be retained until the NRC terminates the license for the reactor.

5. A Licensee Event Report shall be submitted to the NRC within 60 days in accordance with 10 CFR 50.73.

5.3.2 Failure to meet limiting conditions for operation

When an LCO is not met, the following actions shall be taken:

1. The remedial actions permitted by the TS shall be followed, or the reactor shall be shut down until the LCO is met.

2. The failure to meet the LCO shall be reported to the NRC as soon as practical and within 4 hours of occurrence in all cases, in accordance with 10 CFR 50.72.

3. A review of the event shall be conducted, and the results of the review shall be recorded, including the cause of the condition and the basis for corrective action taken to prevent recurrence.

4. A record of the results of the review shall be retained until the NRC terminates the license for the reactor.

5. A Licensee Event Report shall be submitted to the NRC within 60 days in accordance with 10 CFR 50.73.

APPENDIX A: TECHNICAL SPECIFICATIONS BASES

A.1 Safety limit bases

Safety limits for nuclear reactors are limits upon important process variables that are found to be necessary to reasonably protect the integrity of certain physical barriers that guard against the uncontrolled release of radioactivity. If any safety limit is exceeded, the reactor must be shut down. This definition for safety limits and the required action for violation are directly from 10 CFR 50.36(c)(1).

The fuel in the Aurora is a metal alloy of uranium and zirconium, consisting of 90 weight percent uranium and 10 weight percent zirconium. This metal fuel has a melting point (solidus) of 1,200 C [1]. **SL.1** is defined to prevent and minimize the degree of fuel melt in the Aurora. Fuel melt is to be avoided in the Aurora because the fuel significantly loses its capability to retain fission products upon melting. **SL.1** applies to power operation only because that is when the reactor is critical. If **SL.1** is violated, the requirement is to be in hot standby, during which **SL.1** is not applicable. The completion time of 1 hour recognizes the importance of bringing the reactor to a state where the SL is not applicable and reduces the severity of fuel damage.

Many system settings and setpoints are defined such that **SL.1** is maintained, as described in Chapter 2, "Design and analysis of structures, systems and components," of Part II, "Final safety analysis report." These setpoints include those enforced by the reactor trip system (over-temperature, under-temperature, over-power and period too short), and additional trips enforced by the plant control system. All of these trips are intended to enforce the operational limit defined in Chapter 5, "Transient analysis," of Part II, rather than the safety limit. The operational limit is a time-temperature limit that ensures the integrity of reactor cell cans is maintained, and protects against eutectic formation, a phenomenon that is conservatively defined to begin at temperatures above 720 C, and which may not occur unless higher temperatures are achieved.

The analysis of bounding off-nominal events presented in Chapter 5 demonstrated that even during the maximum credible accident, peak fuel temperatures never exceeded 670 C, providing over 500 C of margin to **SL.1**. This transient analysis modeled a reactor trip based on an overtemperature limit setpoint being exceeded. As described, other trip channels provide additional capabilities for detecting off-nominal operation and initiate reactor shutdown, providing defense-in-depth and further ensuring that **SL.1** is met.

Because of the significant margin to the value defined in **SL.1**, limiting safety system settings (LSSS) are not defined in these TS. Section 50.36 to 10 CFR requires the inclusion of LSSS for, "settings for automatic protective devices related to those variables having significant safety functions." The reactor trip system setpoints are the limits of a process variable at which an automated control action is initiated, as established by Chapter 2 of Part II. Change of these setpoints is controlled by 10 CFR 50.59, "Changes, tests, and experiments."

A.2 Limiting conditions for operation and surveillance requirement bases

Limiting conditions for operation are administratively established constraints that ensure that the lowest functional capability or performance levels of equipment required for safe operation of the facility are maintained. The LCOs are maintained by user actions during operation of the facility. Because the Aurora was designed to minimize human involvement during operation, the Aurora has few LCOs.

A.2.1 Shutdown rod system – LCO.01 basis

LCO.01 ensures that the reactor will be shutdown promptly when a reactor trip signal is initiated. The reactor includes three redundant shutdown rods of sufficient worth that only one rod is needed to shut down the reactor from any state. This LCO is an administrative control to ensure design commitment DC.SRS.01is met, as discussed in Chapter 2 of Part II.

The design commitment DC.SRS.02.A commits to a minimum shutdown rod insertion time. Analysis from Chapter 5 of Part II determined that for the bounding transients anticipated for the reactor, the specified shutdown rod insertion time is adequate. This LCO, and the other programmatic controls associated with DC.SRS.02.A, ensure that the shutdown rod system meets the commitment. More details on this commitment, and a further explanation of the basis for it, are in Chapter 2 of Part II.

LCO.01 COND.A ensures that if one shutdown rod fails to insert within the required time, the appropriate measures are taken to restore the shutdown rod system to full capability within 90 days, as required by **TIME.A.1**. **COND.A** is entered if the rod insertion time for one shutdown rod exceeds the allowed time. A 90-day countdown timer automatically begins when **COND.A** is entered. During this 90 day interval, the reactor may be restarted and may continue power operation while arrangements are made to restore the shutdown rod to meet **LCO.01**. The reactor may continue power operation in **LCO.01 COND.A** because two shutdown rods meet the rod insertion time and only one rod is needed to shut down the reactor during any state.

The shutdown rod can be restored to meet **LCO.01** at any time in the 90 day period. After the shutdown rod is restored to meet **LCO.01** and surveillance **SR.01.01** is completed, the 90 day countdown is dismissed by a user action and the plant no longer in **LCO.01**. If the shutdown rod is not restored to meet **LCO.01** in the 90 day interval, the countdown timer expires, a reactor trip is automatically initiated, and **LCO.01 COND.B** is entered.

LCO.01 COND.B ensures that if **LCO.01 COND.A** is not restored in **TIME.A.1**, or if more than one shutdown rod fails to insert within the required time, the reactor is shut down and **LCO.01** must be restored prior to resuming routine power operation. If the rod insertion time for more than one rod exceeds the allowed time, the ability to withdrawal the shutdown rods is disabled because the shutdown rod system no longer has sufficient redundancy. After repairs are made to the restore the shutdown rod insertion time, the ability to withdrawal shutdown rods can be re-enabled by a user action allowing surveillance **SR.01.01** to be performed. Because completion of **SR.01.01** requires testing in the power operation state, the reactor may be operated in power operation for the purpose of completing **SR.01.01**. After surveillance **SR.01.01** confirms that the shutdown rods are restored to meet **LCO.01**, the plant is no longer in **LCO.01.**

SR.01.01 basis: Modifications to the core configuration or the shutdown rod system can change the shutdown rod insertion time. Following any activity that includes removal of the module equipment housing, the rod insertion time shall be verified with cold reactor core conditions and then verified starting from power operation with the reactor core at operating temperature. Following modifications or repairs to address the shutdown rod insertion time that do not include removal of the module equipment housing, the shutdown rod insertion time only needs to be verified starting from power operation.

SR.01.02 basis: Biennial testing of the shutdown rod insertion time starting from power operation with the reactor core at operating temperature ensures the shutdown rods are available to perform their function properly. Surveillance **SR.01.02** can only be performed if the reactor is able to be in the power operation state. If the reactor is not able to be in the power operation state, surveillance **SR.01.02** can be deferred until the reactor can be operated in the power operation state. A written directive signed by the Director of Reactor Operations must be included in the records to indicate the reason for postponement and the expected completion date for the surveillance.

SR.01.03 basis: Unplanned reactor trips during power operations that show the shutdown rod insertion times meet LCO.01 demonstrate that the shutdown rods are available to perform their safety function and may be used to reset the biennial testing interval before the next required surveillance for SR.01.02.

A.2.2. Reactor trip system – LCO.02 basis

LCO.02 ensures that the reactor trip system is functional, which means that it is capable of triggering a reactor shutdown to protect the personnel, reactor, and facility. Reactor trip signals are generated automatically by the reactor trip system or manually by onsite personnel. The reactor trip system automatically generates reactor trip signals in response to the detection of abnormal plant operating conditions or abnormal reactor trip system conditions. Automatic reactor trip signals are initiated in response to the following plant conditions:

- Reactor over-temperature
- Reactor under-temperature
- Reactor over-power
- Reactor period too short

A number of design commitments are made to ensure that both the manual and automatic reactor trips function properly. These design commitments include DC.ICS.01.B, DC.ICS.01.D, DC.ICS.02.A, DC.ICS.03.A, and DC.ICS.04.A. This LCO, and the other programmatic controls associated with these design commitments ensure that the reactor trip system meets these commitments. The analysis of bounding off-nominal events presented in Chapter 5 of Part II determined that if these commitments are met, specifically if the reactor trip system detects an over-temperature condition and sends a reactor trip signal to the shutdown rod system within 6 seconds, the response is adequate to protect the reactor.

The reactor trip system is designed to be fail-safe such that the probable failure modes of reactor trip circuit components will initiate a reactor trip. Reactor trip system conditions that initiate an automatic reactor trip signal include the following:

- Insufficient reactor cell heat pipe temperature channels
- Insufficient reactor power channels
- Insufficient reactor period channels
- Fewer than two functional reactor trip circuits
- Reactor trip circuit bypass switch enabled more than 7 days,
- Failure of a DC power supply within the reactor trip system
- Loss of AC power to the control system

After the reactor has been shut down by the automatic reactor trip system, the cause of the shutdown must be identified. If the reactor was tripped because of a reactor trip system condition, that condition must be resolved prior to startup. Repairs to the reactor trip system require the appropriate surveillance to be completed.

LCO.02 COND.A ensures that if one reactor trip circuit is not functional because a reactor trip circuit bypass switch is enabled, the reactor trip circuit bypass switch is disabled within 7 days, as required by **TIME.A.1**. **COND.A** is entered when a reactor trip circuit bypass switch is enabled. A 7 day countdown timer automatically begins when **COND.A** is entered. During the 7 day interval, the reactor trip circuit bypass switch can be disabled at any time, and the plant is no longer in **LCO.02 COND.A**. If the reactor trip circuit bypass switch is not disabled within 7 days, a reactor trip is automatically initiated, and **LCO.02 COND.B** is entered.

LCO.02 COND.B ensures that if the reactor trip system automatically trips the reactor, either because **LCO.02 COND.A** is not restored in **TIME.A.1** or due to a reactor trip system condition, the appropriate measures are taken to restore the reactor trip system to meet **LCO.02** prior to reactor startup. The plant can be in **LCO.02 COND.B** for an indefinite period of time. Modifications, changes, or repairs made to the reactor trip system to restore the system to meet **LCO.02** may result in one or more surveillance requirements that must be completed prior to startup.

SR.02.01 basis: The reactor trip circuits are designed such that failure of a reactor trip circuit component can cause the reactor trip system to automatically initiate a reactor trip. Redundant reactor trip circuits further ensure that a reactor trip circuit is available to perform the trip circuit function properly. Biennial testing and testing following significant modifications, changes, or repairs to the reactor trip circuits ensures the reactor trip circuits are available to perform their function properly. If the reactor is shut down because one or more reactor trip circuits are not functional, this surveillance cannot be performed. If this surveillance must be deferred, a written directive signed by the Director of Reactor Operations must be included in the records to indicate the reason for postponement and the expected completion date for the surveillance.

SR.02.02 basis: The reactor trip system is designed such that an insufficient number of functional reactor trip system channels will cause the reactor trip system to automatically initiate a reactor trip. Redundant reactor trip system channels are included to reduce the need for a reactor trip because of channel failures. Biennial testing and testing following significant modifications, changes, or repairs to a reactor trip system channel ensures the reactor trip

system channels are available to perform their function properly. If the reactor is shut down because an insufficient number of reactor trip systems channels are functional, this surveillance cannot be performed. If this surveillance must be deferred, a written directive signed by the Director of Reactor Operations must be included in the records to indicate the reason for postponement and the expected completion date for the surveillance.

SR.02.03 basis: Biennial testing and testing following significant modifications, changes, or repairs to the manual reactor trip buttons ensures the manual reactor trip buttons are available to perform their function properly. If one or more manual reactor trip buttons are not operable, this surveillance cannot be performed. If this surveillance must be deferred, a written directive signed by the Director of Reactor Operations must be included in the records to indicate the reason for postponement and the expected completion date for the surveillance.

SR.02.04 basis: The reactor thermal power level channel calibration interval specified in **SR.02.04** ensures that the reactor is operated at the licensed power levels. If the reactor is shut down or the reactor thermal power level channels are not functional, this surveillance cannot be performed. If this surveillance must be deferred, a written directive signed by the Director of Reactor Operations must be included in the records to indicate the reason for postponement and the expected completion date for the surveillance.

A.3 Design feature bases

A.3.1 Reactor system

DF.01.01 basis: The reactor core configuration must be maintained as designed to ensure the validity of the analysis of bounding off-nominal events presented in Chapter 5 of Part II. In addition, this design feature is an administrative control to ensure design commitment SUT.RXS.04.A is met, as discussed in Chapter 2 of Part II.

DF.01.02 basis: Three systems are used to adjust the reactivity of the Aurora core. Two systems, the control drum system and the shutdown rod system, are designed to be active, able to receive command signals and perform mechanical actuation in response. One system, the fixed absorber system, is designed to be manually adjustable during initial core configuration and subsequent maintenance outages. Each of these systems is used to adjust core reactivity according to a different purpose. The purpose of each of these systems is best understood in the context of the others.

The shutdown rod system serves two purposes. First, it provides a means for inserting a large amount of negative reactivity in order to terminate the neutron chain reaction and shut down the reactor. Second, the shutdown rods help add positive reactivity to the core via their slow and controlled withdrawal to compensate for the negative reactivity introduced as the temperature of the core increases during startup from cold conditions. It is the withdrawal of the shutdown rods that compensates for the cold-to-hot negative reactivity worth of the core. The shutdown rods are fully withdrawn from the core once the reactor has completed cold-to-hot heatup and is conducting power operations. Design commitments are taken to ensure that the worth of a single shutdown rod is sufficient to accomplish reactor shutdown over all temperature conditions, including additional margin to account for data uncertainties and reactivity worth changes over life.

The control drum system is designed to compensate for reactivity letdown from fuel depletion during power operations. It is secondarily designed to compensate for the hot zero power to hot full power negative reactivity worth, which is a very small worth due to the very low radial and axial temperature difference across the Aurora fuel during full power operation. The design commitment to limit the combined drum worth to less than 700 pcm was selected to allow the control drum system to compensate for the reactivity letdown with burnup while also setting an upper bound on worth in order to limit the total potential positive reactivity that could inadvertently be added if the control drum system malfunctioned, as analyzed in the transient overpower event in Chapter 5 of Part II.

Finally, the fixed absorber rods are used to reduce initial core reactivity (at cold conditions) such that the other two systems can compensate for the reactivity worth effects for which they were designed to compensate. The fixed absorber rods are configured to ensure that the core excess reactivity is only that which is required to (1) compensate for the cold-to-hot reactivity worth, and (2) compensate for the reactivity loss from fuel depletion.

If neutron cross section data were exact, or operating experience and associated actual reactivity worth data was available, no fixed absorber rods would be required: the initial excess reactivity of the core would be designed to be exactly equal to the sum of the cold-to-hot reactivity worth and the reactivity letdown with burnup. However, due to the presence of cross section data uncertainties and other sources of uncertainty in the reactivity estimates, this ideal situation is precluded at present. As a result, the fixed absorber rods, which are configured during the Initial Test Program as the actual reactivity worths of the system are being characterized, are used to compensate for these uncertainties and allow for adjustment of the initial reactivity of the core. They act almost as a physical "tuning factor" that may be adjusted during this initial core configuration and test period, that then remains fixed in place during operation.

DF.01.03 basis: The reactor systems are designed to ensure a conduction pathway to conduct heat from the reactor core system to the surrounding systems and ultimately to reject to the environment (DC.RXS.04.B). Each of the systems involved in the heat conduction pathway has the appropriated design commitments to ensure that they are installed properly to support heat conduction as described in Chapter 2 of Part II. These design commitments include: the reactor core system (DC.RXS.04.A), reflector system (DC.RXS.05.A), the shielding system (DC.RXS.06.A), the reactor enclosure system (DC.RES.01.A), and the heat exchanger system (DC.HXS.01.A). This design feature is an administrative control to ensure each of these design commitments are met.

A.3.2 Control drum system

DF.02.01 basis: The total reactivity worth of the control drums is designed to limit the effect of an unintended reactivity insertion. This design feature is an administrative control to ensure design commitment DC.CDS.01.B is met, as discussed in Chapter 2 of Part II.

DF.02.02 basis: The control drum drive motors and gearing are designed to limit the maximum rotation speed of the drum to limit the effect of an unintended reactivity insertion. This design feature is an administrative control to ensure design commitment DC.CDS.01.A is met, as discussed in Chapter 2 of Part II.

DF.02.03 basis: The control drum drive actuators are designed to use stepper motors to eliminate the possibility of a hot-short induced unintended continuous rotation. This design

feature is an administrative control to ensure design commitment DC.CDS.01.C is met, as discussed in Chapter 2 of Part II.

A.3.3 Shutdown rod system

DF.03.01 basis: The shutdown rod system is designed with three shutdown rods of equal worth. The rods are suspended above the core by electromagnets such that the rods insert via gravity drop when the electromagnets are de-energized. The simple fail-safe shutdown rod system design ensures the ability to insert shutdown rods into the reactor. The design commitment DC.SRS.02.A commits to minimum shutdown rod insertion time, which is dependent on the proper installation of the shutdown rods as controlled by this design feature.

DF.03.02 basis: The shutdown rod system is designed with three redundant shutdown rods of equal worth, such that each rod can independently provide sufficient negative reactivity to shut down the reactor. The redundant shutdown rod system design ensures the ability to shut down the reactor. This design feature is an administrative control to ensure design commitment DC.SRS.01.A is met, as discussed in Chapter 2 of Part II.

A.3.4 Reactor module placement

DF.04.01 basis: The location and emplacement of the reactor module must be maintained as designed to ensure the validity of the analysis of bounding off-nominal events presented in Chapter 5 of Part II. This design feature is an administrative control to ensure design commitment DC.BAS.01.A is met, as discussed in Chapter 2 of Part II.

DF.04.02 basis: The location of special nuclear material (SNM) in the reactor module, located in the basement of the Aurora facility, ensures the effectiveness of the Physical Security Plan, and Radiation Protection Plan, which both restrict access within the facility as appropriate to protect the SNM in the reactor module. Temporary storage of SNM outside the reactor module is governed by the appropriate maintenance procedures.

A.4 References

[1] G. L. Hofman, L. Leibowitz, J. M. Kramer, M. C. Billone, and J. F. Koenig, “Metallic Fuels Handbook,” Argonne National Laboratory, Argonne, IL, ANL-IFR-29, 1985.

