Response to NRC Request for Supplemental Information Pertaining to Preliminary Safety Analysis Report (PSAR) Chapter 7: Instrumentation and Control, September 27, 2022 (ML22270A177)

October 20, 2022

Prepared by:
Abilene Christian University
Nuclear Energy eXperimental Testing Lab
ACU Box 28208
Abilene, TX 79699-8208

1.1 Request for Supplemental Information 1– Overall I&C Design

Proposed Guidance for Preparing and Reviewing a Molten Salt Non-Power Reactor Application, (ORNL/TM-2020/1478), July 2020, provides guidance for preparing and reviewing a Molten Salt Non-Power Reactor (MSR) Application. Section 7.1, Summary Description, states that the application "should briefly describe the I&C systems of the non-power MSR, including block, logic, and flow diagrams showing major components and subsystems, and connections among them... summarize the technical aspects, safety, philosophy, and objective of the I&C system design and should discuss such factors as redundancy, diversity, and isolation of functions."

Preliminary Safety Analysis Report (PSAR) Chapter 7 Figure 7.2-1 and the related description depicts the architecture of the proposed I&C system. However, the current Figure and description do not provide sufficient detail for the staff to begin the review of the Construction Permit (CP) application.

As a minimum, the Nuclear Regulatory Commission (NRC) staff requests the following supplemental information:

RSI 1.a

- PSAR Figure 7.2-1 and the design description should provide sufficient detail to construct the I&C system in accordance with design principles (redundancy, diversity, and isolation of functions).

RSI 1.b

- PSAR Figure 7.2-1 and the design description should identify outputs from the Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) to end devices, such as actuation of dropping rods, starting pumps, and opening valves to drain MS tank.

RSI 1.c

- PSAR Figure 7.2-1 and the design description should provide sufficient detail on critical communication paths. For example:
    - Communication paths should reflect directionality (one-way or two-way) and any isolation devices (power and classification).

All communication paths should be identified (e.g., those within each safety-related (SR) system, sensor to RPS, sensor to Reactor Control System (RCS), SR to non safety-related (NSR), between Distributed Control System (DCS) and Trip Circuit, manual trip, and offsite).

1.2 Response to Request for Supplemental Information 1- Overall I&C Design

1.2.1 Response to RSI 1.a

Figure 7.2-1 from the CP Application has been updated in Figure 1 below to include sufficient detail of the I&C system and identify outputs from the RPS and ESFAS to end devices. A description of the updated figure follows.

The safety systems of the MSRR are divided amongst two duplicate safety trains. Each safety train additionally utilizes at least one redundant sensor for safety systems, coming to a total of a minimum of four sensors per data point. The physical pathways for cabling and components are isolated between the safety trains, and between the redundant sensors of a particular train as possible.

Additionally, sensors from the Radiation Monitoring System (RMS), utilizing safety rated systems, pass information to the ESFAS, in a similarly redundant manner to each safety train. Sensors and cabling are selected for the conditions present in the MSRR. They are insulated and physically protected, with details of the exact sensor equipment selection, along with protection schemes, planned for the Operating License (OL) application.

The DCS will likely include some degree of redundancy for NSR subsystems in addition to SR ones to allow continued operations in the event of component failure. This redundancy will be oriented towards important subsystems, such as the thermostats for the heating system, to prevent unnecessary thermal cycling. Greater details regarding the exact configuration of the DCS and the vendors chosen to supply it will be provided in the OL application.

The balance of NSR systems required for reactor operation is located in the RCS. In general systems will feature redundant sensors where located in difficult to service areas for operational concerns, but will not be built to the level of reliability expected of SR systems.

It is expected that a data diode may be used to allow outside observation both for oversight and education purposes. Details regarding the data diode will be provided in the OL application.

1.2.2 Response to RSI 1.b

The safety trains encompass both the RPS and ESFAS. An initiation of the RPS does not necessarily initiate the ESFAS. An ESFAS initiation triggers the closing of the auxiliary cooling system louvers and correspondingly necessitates the shutdown of the auxiliary cooling system. As such, for any initiation of the RPS that does not also include detection of radiological release the ESFAS is not triggered to retain the cooling capacity of the auxiliary cooling system. The ESFAS is triggered by detection of a leak or of radionuclide levels outside set points. Any initiation of the ESFAS triggers the RPS as the MSRR relies on the auxiliary cooling system to maintain the limiting conditions for operations related to the reactor cell. Details on why are available in RSI 2.1.

An initiation of the RPS sends a signal to open the trip breakers of the SCRAM system cutting off power to the SCRAM valves, the gas valves between the RAV, the pump bowl, and the drain tank of the fuel salt system. The loss of power causes the SCRAM valves to open, creating a gas connection between the RAV, pump bowl, and the drain tank, equalizing the gas pressure between them and initiating a salt drain. This is described in greater detail in RSI 2.2.

1.2.3 Response to RSI 1.c

Communication isolation between NSR and SR systems is accomplished by isolating individual subsystems on separate communication buses. These separate buses all communicate along bidirectional communication pathways with the control room and the DCS on the facility data bus. The DCS shall be such that communication between NSR and SR systems is regulated appropriately. Unidirectional communication pathways are denoted in Figure 1 by arrows showing the direction of communication. Redundant communication pathways, i.e. communication pathways with multiple physically separate communication lines, are employed between safety system logic controllers, the manual trip, and the trip systems. These pathways are denoted using a separate line type as is indicated in the legend of Figure 1.

2.1 Request for Supplemental Information 2 – Protection of Safety Limits

ORNL/TM-2020/1478, July 2020, provides guidance for preparing and reviewing an MSR Application. Section 7.4, Reactor Protection System, states that the RPS is designed to detect the need to place the reactor in a subcritical, safe shutdown condition (scram) when any of the monitored parameters exceeds the limit as determined in the safety analysis report (SAR). Upon detecting the need, the RPS should promptly and automatically place the reactor in a subcritical, safe shutdown condition (scram) and maintain it there. An MSR scram may include a combination of dumping fuel salt into a drain tank, minimizing reactor fuel flow, or manipulating control elements.

As part of the criteria above, the CP application should provide a system performance analysis of the proposed I&C system to ensure the design criteria and design bases are met and performance requirements of the system are specified, similar to the guidance in ORNL/TM 2020/1478. This should include analysis of any features, aspects, or technical specifications (TS), including surveillance requirements, that may be specific to the reactor and support systems and not identified in the general system requirements. These analyses should be based on postulated credible accidents, transients, and other events that could require RPS intervention, and should include all of the applicable features noted in ORNL/TM-2020/1478, July 2020, Section 7.3 for the RCS. The analyses should include quantitative performance of all scrams, runbacks, interlocks, and ESF initiators.

The staff requests supplemental information on how the objectives of the above paragraphs are met. CP Application Table 7.4-1, Reactor Safety Circuits, describes 10 reactor scram circuits for different conditions to presumably protect safety limits. However, fundamental details needed to begin an evaluation are missing.

RSI 2.a

- Basic details of many functions are missing or are unclear of what are safety limit protections as credited elsewhere in the PSAR versus operational protections. For example, is the safety channel reactor scram for "Temperature" for a high, low, or both setpoint?

RSI 2.b

- When the I&C "scrams" the reactor, it is not clear what is meant from an actuation and safety credit/limit standpoint. The application uses various terms including "SCRAM valves," "system SCRAM," "Reactor scram," "Reactor scram on loss of power," and "protective scram." Are these terms equivalent?

RSI 2.c

The staff also requests supplemental information on when an ESF actuation is required by the accident analysis. The description in PSAR Section 7.5 states "[t]he ESFAS is designed to trigger in all credible accident scenarios." Is ESF actuation initiated under all scenarios examined under PSAR Table 13.2-1?

2.2 Response to Request for Supplemental Information 2 - Protection of Safety Limits.

2.2.1 Response to RSI 2.a

SCRAM channels and triggering values are listed in Table 1 and then discussed in greater detail, covering both the trigger points, safety limits, and how they will be monitored in subsequent paragraphs. This table is intended to replace CP Application Table 7.4-1.

Table 1. *SCRAM channels alongside trigger values and references to PSAR sections explaining why those values were selected.*

SCRAM System Channel	Triggering Values	Ref.
Reactor Power	~1.0 MWth	14.2.2
Fuel Salt System Temperature (FSST)	~550 °C < FSST < 650 °C	4.3.8, 14.2.2
Coolant Salt System Temperature (CSST)	~550 °C < CSST < 650 °C	4.3.8, 14.2.2
Fuel Salt Level (FSL)	Below the gas management system (GMS) piping level and above the top of the salt outflow pipes	4.3.11, 14.3.1
Coolant Salt Level	Below the gas management system (GMS) piping level and above the top of the salt outflow pipes	4.3.11, 14.3.1
Fuel Salt System Gas Pressure (FSSGP)	0.1MPa < FSSGP < 0.5 MPa	4.3.7, 14.2.2
Coolant Salt System Gas Pressure (CSSGP)	0.1MPa < CSSGP < 0.5 MPa	4.3.7, 14.2.2
ESFAS Initiation	N/A	14.3
Manual Trip	User initiation	7.6.2
Loss of Neutron Detector High Voltage	TBD	7.4.6
Loss of Power to Console/Detected Fault	TBD	7.4.6
Loss of RMS or Components	TBD	7.4.6
Key Switch	N/A	7.4.6

Reactor thermal power is a limiting safety system setting, and limiting condition of operation. In none of the analyzed accidents were power excursions significant enough to approach the safety limits. Reactor thermal power is monitored by four calibrated detectors on two trains. Reactor power level trip point will be set in the OL application when greater information regarding measurement accuracy and system response time will be available. It will be chosen to protect the licensed power level and is expected to be nominally 1 MWth.

The temperatures of the salt systems are safety limits. The different salts in the fuel and coolant salt systems may lead to differing operational and safety limits. The high temperature operational and safety limits are set by the limiting temperature of the steel used to construct the salt systems. The safety limit for the steel is 816 °C, with an operation limit of 650 °C set to protect that limit. The low temperature safety limit is set by the salt freezing point, for which the precise values are unknown. They are expected to be < 500 °C and so operational limits are nominally set at 550 °C. Differences in the freezing points may lead to different low temperature operational and safety limits for the different salt systems. The final limits will be set in the OL application when greater details on the properties of fuel and coolant salt are available. During system shutdown, or low power operations not requiring the primary heat removal system, the temperature of the system will normally be controlled by the system thermostats, which will have control of the electrical heaters for the system. In order to minimize system thermal cycles, the thermostats will maintain the system operation temperature of 600 °C routinely, only cooling the system for maintenance, or protective actions. For power operations above approximately 10 kWth it is expected that the primary heat removal system will need to be activated to maintain thermal limits. The precise system thermal behavior will be described in the OL application. During a SCRAM power to the heaters is cut by the trip breakers to prevent system overheating in the event of an unexpected malfunction. The system temperature will be monitored by a network of thermocouples with redundant sensors on two separate trains in keeping with the facility safety approach. The precise arrangement and number of thermocouples deployed to monitor the system will be available in the OL application.

Salt level in the fuel salt and coolant salt systems is a limiting condition of operation. The GMS is not designed to withstand salt intrusion, and as such the salt level must be kept below the level of the GMS system openings in the salt systems. Additionally, during power operations involving the primary heat removal system, the salt level in both systems must be sufficiently high to establish a circulation loop, to prevent salt stagnation or restricted ability to cool the salt. Correspondingly there is a minimum salt level requirement above the level of the outflow pipes from the fuel salt loop's RAV, and pump bowls, and from the coolant salt loop's expansion tank and pump bowl. The salt levels in the RAV, the pump bowls, and expansion tank will be monitored to ensure the salt levels remain within the proscribed operational limits for the current operation state of the MSRR. The salt level monitoring will be accomplished by four salt level sensors each on two separate trains with more detail on precise sensor selection and operation in the OL application.

The pressure in the fuel salt and coolant salt systems is a safety limit. It is set by the mechanical properties of the system vessels and piping, and takes into account the behavior of radionuclides during potential accidents. The safety limit for both the fuel and coolant salt systems will likely be between 0.1 and 0.5 MPa. These limits will be finalized as part of the detailed engineering design included with the OL application. The system pressures will be monitored at the location of limiting system pressure, which is expected to be the salt drain tanks, the RAV, expansion tank, and pump head spaces. During a SCRAM the pressure supply will be isolated to prevent a system overpressure in the event of an unexpected malfunction. The pressures will be monitored using redundant

pressure sensors on two trains. Details of sensor selection and operation will be in the OL application.

The initiation of the ESFAS always triggers the RPS. The auxiliary cooling system's cooling air serves both to protect the mechanical properties of the materials that comprise the reactor cell, and to maintain the initial conditions of any accident analysis. The accident analyses show that, starting from the temperature profile maintained by the auxiliary cooling system, the system retains sufficient thermal inventory to absorb and dissipate any heat from a hypothetical accident. Because the activation of the ESFAS restricts the flow of cooling air, any additional power operation after ESFAS initiation will place the system outside the initial conditions of the accident analyses. Therefore, to maintain the conditions upon which the accident analyses were performed the RPS must always initiate and bring the reactor to a shutdown state following ESFAS initiation.

A manual trip signal will be passed along redundant communication pathways to the SCRAM trip breakers to ensure reliability. The communication pathways will be physically separated, as all SR pathways are, as much as possible.

Neutron detector high voltage passing outside of the acceptable range for operation of the detection system will trigger a scram, potentially after an appropriate time delay. Greater detail on the specific sensors selected and the exact triggering details will be available in the OL application.

A detected fault in the control console or a loss of power will trigger a SCRAM. Greater detail regarding the specifics of the console design and operation will be available in the OL application.

A loss of SR RMS detectors will trigger a SCRAM, potentially after a time delay. As the ESFAS can potentially initiate based on readings from the RMS, a loss of the RMS must default to an ESFAS initiation and correspondingly a SCRAM. A time delay in this initiation may be allowable and will be discussed based on further safety calculations and consideration of response time in the OL application.

2.2.2 Response to RSI 2.b

The term "SCRAM valves" refers to the gas equalization valves used to affect a salt drain. The terms "system SCRAM," "Reactor Scram," "protective scram" are all equivalent, and describe activation of the MSRR SCRAM system, which is comprised of the gas equalization valves used to affect a salt drain, the trip breakers controlling power to those valves, and the controllers/initiators for those breakers. A "Reactor scram on loss of power" is the natural consequence of the fail-safe nature of the gas equalization valves, which upon loss of electrical power open, triggering a fuel salt drain. The SCRAM system and process along with the controlling devices and logic is described in greater detail below.

The RPS is a distributed system with initiating devices executing the SCRAM logic present on both safety trains. Signals from the safety sensor pairs will pass through the RPS controllers on their way to the DCS and the control room. If any one of the signals violate set limits, a SCRAM signal will be sent to the trip breakers initiating a SCRAM. This will occur if any single sensor signal violates a limiting value. As with all safety systems in the MSRR this will be accomplished by a minimum of two separate signal pathways traveling along physically divided paths as much as possible. Cabling

suitable for the MSRR will be utilized and will be physically protected to meet the MSRR firefighting and accident plans.

The MSRR accomplishes a reactor SCRAM through the exclusive use of gas valves. The control rods of the MSRR will only be utilized for controlling the power level of the reactor during normal operation as part of the RCS, playing no part in a SCRAM. Upon RPS initiation, signals passed along redundant cabling pathways will open the trip breakers for the SCRAM system. This will cut off electrical power to the four SCRAM gas valves. The SCRAM valves consist of four valves on two gas lines. The number of valves and lines is chosen for reliability and diversity, the opening of any one valve on either gas line is sufficient. Upon the loss of power, the four valves will open connecting the gas volumes between the RAV, the fuel salt pump head space, and the fuel salt drain tank. This will equilibrate the gas pressure immediately resulting in the beginning of a fuel salt drain out of the reactor loop into the drain tank. Two drain lines connect the reactor vessel to the drain tank for reliability and diversity. Because the reactor vessel, the two fuel salt drain lines, and the drain tank are all contained inside the thermally insulated boundary of the RTMS fuel salt will remain molten for the period required to drain. Once the reactor vessel reaches ¾ full the system will become subcritical. After one minute the fuel salt level will be below the level of the reactor vessel graphite. Because the fuel salt is held in place by gas pressure a gas pressure leak will have the same effect as a SCRAM and drain the fuel salt into the drain tank. Once the fuel salt inventory has relocated to the drain tank the reactor is in a shutdown state. Under no credible accident investigated can the drain tank become critical. Upon SCRAM initiation power to the system heaters is interrupted along with isolation of pressured cover gas to prevent potentially exceeding safety limits in the event of an unanticipated malfunction.

2.2.3 Response to RSI 2.c

The ESFAS brings the MSRR into a configuration that meets the designed leak rate of the system for potential accidents. It does this by sealing the air passages to and from the reactor cell air space, and by sealing valves on all gas penetrations through the reactor enclosure. The reactor cell air passages contain louvers capable of achieving the designed system leak rate. Following the receipt of an ESFAS signal the louvers will be closed by fail safe drives. The drives will be such that the loss of power brings the louvers to the sealed position. The enclosure penetrating gas lines will all feature at least a pair of valves, each rated to independently isolate the line. The valves will be fail safe such that in the event of a loss of power the valves seal the system to its designed accident configuration. The exact selection of louvers, the louver drives, and gas valves will be available in the OL application.

The ESFAS initiation is prompted by the detection of a failure in one of the fission product barriers, or the detection of elevated radionuclide concentrations outside of fission product barriers. The precise logic used to determine the failure of a fission product barrier will be included in the OL application, but it is expected to include the detection of sudden changes in pressure indicative of a line failure. Additionally, signals from RMS sensors on safety rated redundant trains will be passed to the ESFAS as monitoring for the potential release of radionuclides. A manual initiator will be included in the controls present in the control room.

The ESFAS is a distributed system with initiating devices executing the ESFAS logic present on both safety trains. Signals from the sensor pairs will pass through the ESFAS controllers on their way to the DCS and the control room. If any of the signals violate set limits a ESFAS signal will be sent to the trip breakers bringing the system to its designed accident configuration. As with all safety systems

in the MSRR this will be accomplished by a minimum of two separate signal pathways traveling along physically divided paths as possible. Cabling suitable for the MSRR will be utilized and will be physically protected to meet the MSRR firefighting and accident plans.

3.1 Request for Supplemental Information 3 – Principal Design Criteria for I&C and Design Standards

A CP application needs to provide principal design criteria (PDCs) that are applicable to the I&C system with respect to its function in safe reactor operation and shutdown, and response to anticipated accidents and analyzed accidents. The application would also reference applicable codes and standards that will be achieved. The PSAR narrative would subsequently describe the key design attributes that will be relied upon to address those PDCs

PSAR Chapter 3 provides PDCs, as applicable to the ACU I&C system. However, the staff requests the following supplemental information that could impact I&C system design:

RSI 3.a

- PDC 19 states that equipment at appropriate locations outside the control room shall be provided with a design capability for safe shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition and allow for interventions such as fuel loading, inspection, and repair. However, there is no fundamental discussion of this alternate shutdown location in the PSAR.

RSI 3.b

- PDC 21 states that no single failure results in loss of the protection. However, there is no fundamental discussion of how "Individual components of the RPS can be removed from service for testing without loss of required minimum redundancy" can be accomplished in the PSAR.

RSI 3.c

- It is not clear if PDC 26 is applicable to RCS. PSAR Section 7.3 does not list PDC 26, while PSAR Section 4.2.2.2 identifies PDC 26, and states "the RPS in conjunction with the RCS provide separate and diverse means for controlling reactivity changes." The discussion of PDCs and respective function/credit of I&C needs to be consistent throughout the PSAR.

3.2 Response to Request for Supplemental Information 3 - Principal Design Criteria for I&C and Design Standards

3.2.1 Response to RSI 3.a

Upon re-examination of PDC 19 it was determined to be inapplicable to the MSRR. Based on the safety analysis no accidents have been identified that require controls outside the bounds of the control room. More details regarding the emergency plan will be available in the OL application.

The requirement to have controls for safe shutdown and intervention outside the control room is deemed unnecessary and PDC 19 will be deleted.

3.2.2 Response to RSI 3.b

Upon re-examination of PDC 21 it was determined that the in-service testability requirements were excessive for the MSRR. As a research reactor there are no requirements for continual operation that make in-service testability necessary. Testing will be performed with the reactor in conditions for which there is no possibility of a single failure, with greater details included in the OL application. The in-service testability requirements will be removed from PDC 21.

3.2.3 Response to RSI 3.c

PDC 26 was inadvertently left out of PSAR section 7.3. It is intended to describe the functionality of the RCS and will be included in all future documentation.

Figure 1 - I&C System