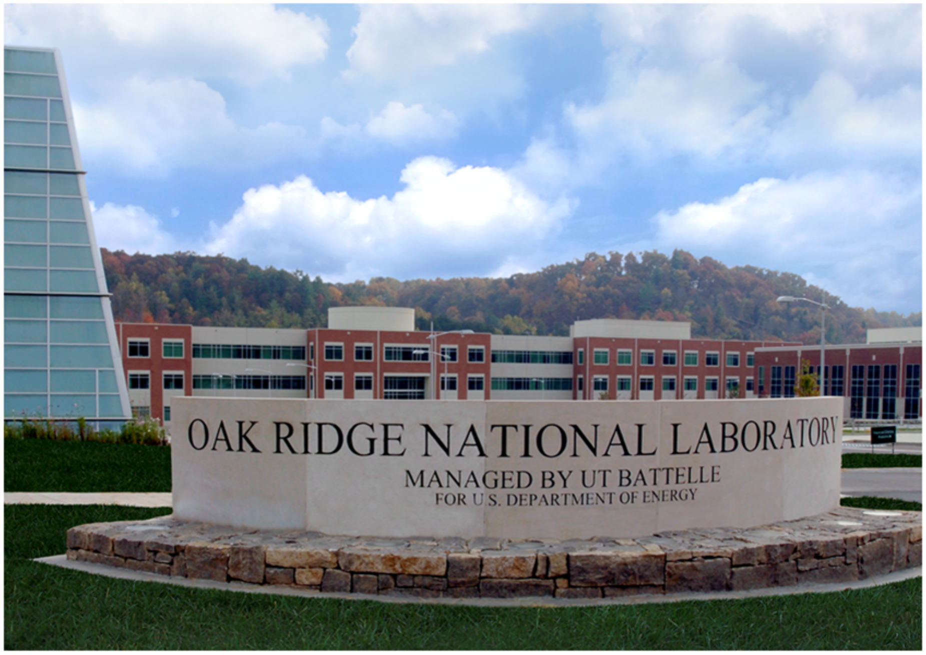
ORNL/SPR-2019/1254
TCR-RG-RPRT-002

Safety Design Strategy for the Transformational Challenge Reactor



Stuart Severns

August 2019

M2CT-19OR06090141

ORNL/SPR-2019/1254
TCR-RG-RPRT-002

Transformational Challenge Reactor

Safety Design Strategy for the Transformational Challenge Reactor

Stuart Severns

M2CT-19OR06090141

Version 0
August 2019

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831-6283
managed by
UT-BATTELLE, LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

Abstract

The Department of Energy Office of Nuclear Energy is embarking on the Transformational Challenge Reactor (TCR) program to demonstrate application of advanced technologies in enabling rapid and cost effective deployment of nuclear power systems. The TCR program will design, manufacture, and operate a small nuclear reactor at the Oak Ridge National Laboratory incorporating advanced manufacturing. DOE Order 420.1C requires the integration of safety in the design process. Therefore, the general approach in DOE-STD-1189 as described in this Safety Design Strategy is applied to the project to establish requirements for safety design for the resultant Categorized Nuclear Facility/Activity and to ultimately allow the Department of Energy to authorize operation of the facility.

Contents

Tables

Acronyms

ASME	American Society of Mechanical Engineers
BEU	Beyond Extremely Unlikely
CM	Configuration Management
COR	Code of Record
DBA	Design Basis Accident
DID	defense-in-depth
DOE	U.S. Department of Energy
DSA	Documented Safety Analysis
HALEU	high-assay low enriched uranium
MHA	Maximum Hypothetical Accident
NCS	Nuclear Criticality Safety
NEPA	National Environmental Policy Act
NPH	Natural Phenomena Hazards
NRC	U.S. Nuclear Regulatory Commission
ORNL	Oak Ridge National Laboratory
PDSA	Preliminary Documented Safety Analysis
QA	Quality Assurance
SAC	Specific Administrative Control
SC	Safety Class
SDS	Safety Design Strategy
SME	subject matter expert
SMP	Safety Management Program
SS	Safety Significant
SSC	structures, systems and components
TCR	Transformational Challenge Reactor
TED	Total Effective Dose
TSR	Technical Safety Requirement
TQ	Threshold Quantity

1. PURPOSE

Consistent with U.S. Department of Energy (DOE) standard DOE-STD-1189-2016, "Integration of Safety Into the Design Process,"[1] this Safety Design Strategy (SDS) for the Transformational Challenge Reactor (TCR) program at the Oak Ridge National Laboratory (ORNL) describes the overall approach to nuclear safety, describes the strategy for safety-related design decisions, identifies key assumptions or inputs that may represent potential risks to design decisions, and identifies expected safety basis deliverables throughout the project. Requirements for the integration of safety in the design process from DOE O 420.1C "Facility Safety"[3] will be applied on a graded approach. Safety analysis documentation will meet the requirements of 10 CFR 830[4], "Nuclear Safety Management," Subpart B, "Safety Basis Requirements."

2. DESCRIPTION OF THE PROJECT

The TCR program is a multi-year demonstration effort to deliver a paradigm-changing design and manufacturing template for the nuclear power industry. The program will integrate areas of high technology research including high-performance computing, data science, machine learning, and advanced manufacturing to accelerate design, testing, optimization, and qualification of nuclear reactor components. To demonstrate the efficacy of this integrated concept, the program will design, build and conduct a short operational test of a microreactor with features within the reactor core that are only possible through use of advanced manufacturing. To quickly capture the benefits to the nuclear industry, the program is targeting an aggressive timeline to begin startup activities in 2023.

The pre-conceptual physical characteristics of the TCR design envelope are as follows:

- Fuel Type: High Assay Low Enriched Uranium (HALEU) as UC, UO_2, UN, or their mixtures
- Fuel Mass: < 250 kg total U
- Core Structure: 316 SS and SiC
- Vessel: 304H SS
- Reflector: Graphite or water
- Moderator: Yttrium hydride
- Coolant: Pressurized He
- Control: B_4C (drums/rods/elements)

The TCR operational envelope is as follows:

- Power: < 6 MWth
- Power Density: < 30 W/cc
- Outlet Temperature: < 550 °C
- Primary System Pressure: < 8.0 MPa
- Operating Life: < 24 hour full-power equivalent

As design constraints are identified and finalized, conventional equipment items will be specified, and procurement of long-lead items will be initiated as allowed by 10 CFR 830.206(a)(2). National Environmental Policy Action (NEPA) assessments will be completed, and the Building 7709 will be made ready to accept the reactor and associated systems.

Principle construction activities and the reactor proposed location is Building 7709 on Copper Ridge, across Melton Valley from the main ORNL campus in Bethel Valley. This building formerly housed the Health Physics Research Reactor which was operational between 1963 and 1987. A control room is located in a remote building (Building 7710) about 0.25 km east southeast of the reactor building. A modular TCR control station is proposed and will be located adjacent to Building 7710.

Prototypes of the advanced-manufactured core will be evaluated though testing and non-destructive and destructive characterization techniques. The program will also rely on a digital platform that will be built to collect as-built manufacturing data and perform quality assessments. The digital platform will incorporate feedback from testing and characterization and undergo software quality assurance. Components outside the core will use traditional manufacturing compliant with established standards.

The reactor core will include embedded sensors to collect reactor health and performance. However, a traditional analog safety protection system will be relied on for safety functions.

Authorization by DOE will be sought prior to assembly of the reactor, systems pre-startup testing, and reactor operation. After completion of the short-duration operational test, the reactor will be deactivated and decommissioned, and post-operation characterization activities will be performed. Operational data collected via sensors embedded in advanced manufactured items will provide additional feedback to the design platform for future refinement. The core will be removed for characterization and transport after the requisite cooldown period. The long-term management of the irradiated core and other components is not anticipated.

3. PROCESS ASSUMPTIONS

Although the TCR program ultimately results in the brief operation of a small nuclear reactor, the relative time-at-risk for a significant source term is orders of magnitude shorter than for a typical enduring nuclear facility. Regardless, the design criteria and safety design approach will be conservatively applied but will be graded based on the short duration of risk exposure, and the limited amount of time safety systems are required to maintain their safety function.

The TCR design criteria and design processes where applicable will be consistent with DOE O 420.1C, Nuclear Regulatory Commission (NRC) Regulatory Guide 1.232, “Guidance for Developing Principal Design Criteria for Non-light-water Reactors”[5], and ASME NQA-1-2008 (and 2009 addendum)[6]. Current relevant process assumptions regarding design criteria and design processes are as follows:

- Maximum operational duration of the TCR shall not exceed 24 hour full-power equivalent (safety design basis value).
- Reactor and auxiliary SSCs shall incorporate inherently safe features commensurate with assessed risk.
- Reactor active-engineered controls shall be fail-safe.
- Existing structures/design features are assumed to not conform to current Natural Phenomena Hazards (NPH) design criteria.
- Reactor vessel, piping, heat exchangers shall conform to existing American Society of Mechanical Engineers (ASME) Boiler and Pressure Vessel Code, Section III[7] requirements or equivalent approved codes and standards.
- Reactor vessel and associated safety SSCs shall be designed to perform their safety function during and following a design basis seismic event (including structural collapse of the building).
- Reactor vessel shall be designed to maintain a confinement safety function during a design basis tornado/high wind event.

Given the uniqueness of the TCR program, the regulatory regime dictates a similarly unique approach. Safe Harbor Documented Safety Analysis (DSA) development methodologies given in 10 CFR 830 are judged not well suited for the TCR program. Therefore, an alternate approach has been proposed using applicable elements of NRC NUREG-1537, "Guidelines for Preparing and Reviewing Applications for Licensing of Non-Power Reactors"[8] incorporating relevant aspects of DOE O 420.1C as implemented by DOE-STD-1189-2016. The result of the TCR program will be a new nuclear facility, and there are no identified interfaces with existing nuclear facility safety basis documents. Current relevant process assumptions regarding development of the safety basis are as follows:

- DOE Site Office is the regulatory approval authority.
- DSA format and content shall be consistent with NUREG-1537.
- Evaluation Guidelines and consequence thresholds shall be consistent with DOE-STD-3009-2014[9] with the exception of acute intake of uranium (if considered).
- Toxic uranium intake (if considered) shall be in accordance with NRC FCSE Interim Staff Guidance ISG-14, "Acute Uranium Exposure Standards for Workers"[10].
- Selection and functional classification of safety controls shall be consistent with DOE standards and guidance.
- Facility worker access to the facility shall be administratively controlled [i.e., a Specific Administrative Control (SAC)] to preclude exposure to all hazards but those when workers are necessarily present (e.g., core handling/installation/ removal and testing activities).
- Operation of the TCR shall be precluded if severe weather is probable.
- Collocated worker locations are the control room station (i.e., ~250 m), nearest point of site access restriction, and/or nearest normally occupied facility.
- The TCR operational personnel will be drawn from the pool of qualified staff at the High Flux Isotope Reactor or the Nonreactor Nuclear Facilities Division.

- Direct radiation exposure to collocated worker considers physical features (e.g., earthen separation) to be present for postulated direct exposure hazard scenarios.
- Frequency of design basis NPH events while the TCR is operating is considered Beyond Extremely Unlikely (BEU).

Given the limited operational duration of the TCR, major programmatic contributors to safety are Safety Management Programs (SMPs) that provide safety assurance in the design, construction, and start-up phase of the program. Consequently, the approach to SMPs will be graded based on importance to early life cycle performance. Programs such as Quality Assurance (QA), Conduct of Operations (testing/readiness type of activities) will have a higher weighting in the safety basis. SMPs such as Radiation Protection, Safeguards and Security, and Emergency Response will be in accordance with existing ORNL programs.

SMPs focused on longer-term safety assurance such as the Configuration Management (CM) Program will focus more heavily on design configuration control and verification of as-built conditions. Beyond compliance with 10 CFR 830 and NQA-1, QA and CM plans and implementation strategies are evolving as the program matures. Similarly, the Code of Record (COR) and management of same is evolving and will be consistent with DOE standards and guidance.

Given the relative simplicity, accelerated design timeline, and short operational duration of the TCR, a graded safety basis development framework consistent with 10 CFR 830 is proposed. The SDS will be periodically updated to document significant safety design decisions and/or changes in safety control strategy as they are finalized. When a mature design envelope and control strategy is established, a Preliminary Documented Safety Analysis (PDSA) will be developed for DOE approval. Following PDSA submittal, a robust change management system will control the safety design such that the delta from the PDSA is clearly documented. When design is certified for construction, the Documented Safety Analysis (DSA) and associated Technical Safety Requirements (TSRs) will be finalized and submitted for DOE approval.

4. SAFETY SYSTEM SUPPORT INTERFACES

Support and infrastructure systems may be required for safety system operation. Major facility interfaces critical to design and the safety design will be reviewed. In particular, a structural evaluation of Building 7709 and control system support structures will be performed to assess existing NPH resistance. For the purposes of the SDS though, it is assumed the facility and support system interfaces of existing building structures do not meet current design basis NPH requirements. Although it is noted above the reactor and associated safety SSCs will be designed to perform their safety function during and following a design basis seismic event, it is also possible the building structure may be upgraded to meet seismic design requirements, if judged feasible. It is unlikely the building structure would provide adequate protection against wind driven missiles under a design basis wind event; therefore, the reactor vessel will be designed to maintain a confinement safety function under such conditions. Regardless, the reactor will administratively be placed in a safe condition upon notification of potentially severe weather.

Given the above discussion, the following general criteria will be utilized to designate and perform functional classification of safety systems:

1. In general, system interactions will be addressed by upgrading, where feasible, non-safety SSCs to the extent necessary to preclude adverse interaction with safety SSCs. Where upgrades are not feasible, safety SSCs will be designed to continue to perform the safety function when exposed to the adverse interaction.

2. Reactor control and safety systems interface via physical signal cabling between Building 7709 and the TCR control station. Cable trays run above ground between the buildings on support structures. Adverse interaction with the outdoor environment will be assessed and appropriate action taken to preclude adverse interaction under normal and credible abnormal conditions. Safety systems will be designed to fail safe on loss of control signal. Furthermore, the reactor will administratively be placed in a safe shutdown condition upon notification of potentially severe weather.

3. Electrical power is supplied via overhead power distribution to both Building 7709 and the TCR control station. Offsite power will similarly be assessed for adverse environmental interactions and action taken to preclude adverse interaction under normal and credible abnormal condition. Safety systems will be designed to fail safe on loss of power. The need for backup power will be assessed as the design matures.

4. Onsite support systems necessary for safety SSCs to perform a safety function will receive the same functional classification as the safety SSC. If backup power is required, it may require functional classification.

5. SAFETY STRATEGY

The overall safety strategy for the TCR program will be substantially similar to that of a typical DOE or other experimental/research reactor. The proposed strategy will, however, apply a graded-approach based on short operational duration (i.e., relatively small fission product source term). As previously described, the design and manufacturing of the reactor core and possibly other reactor components will be novel. Although, the QA program may be similarly novel, the program will be developed and implemented in accordance with NQA-1-2008 (and 2009 addendum) and standards as applicable. Therefore, a safety design initial condition is the QA program/approach shall appropriately procure and qualify reactor components and support equipment in accordance with an approved TCR QA Plan.

The TCR program safety design will utilize NRC Regulatory Guide 1.232, "Guidance for Developing Principal Design Criteria for Non-Light-Water Reactors" to develop TCR design criteria. NRC General Design Criteria given in 10 CFR Part 50, Appendix A[11], may also be considered in the safety design as applicable.

The preliminary initial hazard categorization is assigned consistent with DOE-STD-1027-2018[12], "Hazard Categorization of DOE Nuclear Facilities". Per the standard, TCR is a Category B Reactor as the power level is less than 20 MWth. Since the TCR is not a Category A reactor and has not been designated a Nuclear Hazard Category 1 facility, the SDS preliminarily categorizes the TCR as Nuclear Hazard Category 2. The TCR will by definition have the potential for nuclear criticality. As such, Nuclear Criticality Safety (NCS) controls will be required for activities associated with the storage and handling of the reactor core. NCS controls may require incorporation into the TSRs based on programmatic requirements. If the potential for nuclear criticality can be precluded by nature of the process or by segmentation, the provision for step-out from hazard categorization may be provided in the DSA.

A comprehensive safety analysis of the TCR will be performed and documented in a DSA consistent with 10 CFR 830. An alternate methodology for preparing the DSA is proposed. The proposed DSA format and contents will be consistent with NUREG-1537. A preliminary description of DSA content is presented in Appendix A. A reasonably conservative qualitative approach to hazard/risk analysis consistent with NUREG-1537 and DOE G 421.1-2A, "Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830"[13] is proposed. Qualitative aspects of the hazard analysis will be supplemented by quantitative or semi-quantitative analyses as necessary to assure qualitative conclusions are conservative.

Dose consequences for applicable Design Basis Accidents (DBAs) as well as a Maximum Hypothetical Accident (MHA) as described in NUREG-1537 will be determined in the safety analysis. Accident consequences will be used to assess the risk of lesser postulated events identified in the hazards analysis and will guide the functional classification of identified preventive and mitigative controls.

Consistent with DOE guidance, the hierarchy of controls will be utilized. Preventive controls are selected over mitigative controls. Passive controls are selected over active controls. Engineered controls are preferred over administrative controls. However, given the limited operation of the reactor, significant investment will not be justified to eliminate effective administrative controls.

The goal of safety analysis is to analyze potential accidents and to protect the public, workers, and the environment through the identification and selection of both physical and programmatic controls. Selected controls prevent and/or mitigate analyzed accident consequences to acceptable levels of residual risk. In addition to the hierarchy of controls, a defense-in-depth (DID) strategy consistent with DOE standards and guidance will be implemented which relies on several layers of protection to prevent the release of radioactive or hazardous materials. Controls selected will apply redundancy and/or independence of operation where necessary such that no one layer is exclusively relied upon.

The first layer of DID relies on a high level of design quality such that passive SSCs are capable of preventing the release of radioactive material. Based on the current conceptual design, TCR passive containment SSC are preliminarily identified as follows:

- Fuel properties and cladding/core structure
- Reactor vessel
- Coolant loop

As discussed above, a novel design and manufacturing approach is central to the program. Programs to assure equipment quality and resultant safety will be important. Programs including QA and pre-start up testing and readiness will assure that TCR SSCs are capable of performing the required safety function prior to operation.

The second layer of DID ensures that if the intended safety function of the first layer is compromised, additional controls are available to prevent the progression of an accident sequence. Controls in the second layer consist of automatic or manual controls and operator actions to place the systems in a safe configuration. TCR controls preliminarily identified in this layer are as follows:

- Reactor control drums/rods/elements
- Plant control system
- Reactor protection system

The third layer of DID provides for the mitigation of consequence if an accident were to occur. Consistent with the proposed graded approach, much of the third layer of protection consists of administrative controls. Administrative controls are relied upon to control access to the immediate vicinity of the TCR and implement appropriate emergency response. Following are the preliminary controls identified in the third layer:

- TCR operational duration control
- Site security/access control
- System confinement/ventilation system
- Radiation protection
- Emergency response

Functional classification of controls will be in accordance with DOE standards and guidance. SC functional classification is assigned when controls and required support system are credited for preventing/mitigating accidents with the potential to exceed the Evaluation Guideline [25 rem Total Effective Dose (TED)]. Safety Significant (SS) functional classification will be assigned when controls and required support systems are credited for preventing/mitigating accidents with the potential to challenge the EG (greater than or equal to 5 rem TED) or exceed the collocated worker threshold of 100 rem TED. Facility worker consequences will be qualitatively assessed. The Radiation Protection Program will control worker exposure for normal operations and maintenance activities. Administrative controls assessed to perform a SC or SS function will be designated as Specific Administrative Controls (SACs). DID controls identified to provide significant protection to the on-site workers will also be consider for risk-informed SS functional classification consistent with DOE standards and guidance.

As previously discussed, the TCR operational duration is short compared to a DOE nuclear facility with an enduring mission. As a result, the TCR time-at-risk may not justify significant expense and effort to upgrade existing facilities and structures to meet current NPH design requirements as required by DOE O 420.1C. It is expected the safety analysis will specify a safety design consistent with DOE risk acceptance criteria. Safety controls and required support systems will be designed and specified consistent with DOE O 420.1C.

Air dispersion modelling will be performed consistent with DOE guidance and standards. DOE toolbox codes will be used to assess radiological dose to receptors of interest.

6. SAFETY GUIDANCE AND REQUIREMENTS

Numerous sections of the CFR, DOE Orders and other policy requirements may apply to the design, construction, and operation of the TCR. Key drivers for the development of the safety/authorization basis for the TCR program are briefly described below.

10 CFR 830 Subpart B "Nuclear Safety Management" is the regulatory driver for the development of a DSA for DOE categorized nuclear facilities. The DSA ensures hazard controls are established to provide for the adequate protection of workers, the public, and the

environment. TSRs are required to be derived from the DSA. The TSRs establish limits, controls, and required actions that establish specific parameters and requisite actions for the safe operation of nuclear facilities. For new nuclear facilities, a PDSA must be prepared.

DOE O 420.1C "Facility Safety" establishes facility and programmatic safety requirements at DOE facilities for nuclear safety design criteria, fire protection, nuclear criticality safety, NPH mitigation, and a cognizant systems engineering program. Elements of the Order are typically implemented site-wide via programs, such as fire protection program, criticality safety program, etc. TCR-specific issues for each element are briefly described as follows:

Nuclear Safety Design Criteria

The Order requires the integration of safety with design. Use of DOE-STD-1189-2016 is specified. The standard provides requirements and guidance for integration of safety in design. Development of safety basis documents, including the SDS, is described in the standard. The standard is proposed to be applied on a graded-approach; specifically, proposed program safety basis documents are the SDS, PDSA, and DSA/TSR.

Based on initial scoping calculations, hazards associated with the TCR have the potential to exceed the EG. As a result, the following invoked Institute of Electrical and Electronics Engineers standards may apply to the TCR:

- IEEE 379-2014, "IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems"[14]
- IEEE 323-2003 (R2008), "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"[15]

Many of the Advanced Reactor Design Criteria and modular High Temperature Gas-cooled Reactor (mHTGR) design criteria specified in RG. 1.232, "Guidance for Developing Principal Design Criteria for Non-light-water Reactors" are applicable to the TCR and will meet the safety philosophy of the general design criteria specified in DOE 420.1C. From these sources, TCR principal design criteria will be developed. An example of a preliminary set of design criteria (for one reactor design currently under consideration) is presented in Appendix B.

Fire Protection

It is anticipated, the TCR will require no more than programmatic controls (e.g., combustible loading) related to fire protection. Building 7709 does not contain a fire sprinkler system. A fire water riser is located near the building. A Fire Hazards Analysis will be performed for TCR activities.

Nuclear Criticality Safety

The TCR program includes the operation of a small, fission reactor. TCR-specific NCS analyses will be performed to specify controls for activities involving core storage and handling while outside the reactor.

NPH Hazard Mitigation

The Order requires facilities to be designed, constructed, maintained, and operated to ensure SSCs will be able to perform intended safety functions under design basis NPH conditions as specified in applicable building codes in the facility COR. The Order specifies the use of the design requirements and criteria in DOE-STD-1020-2016[16], "Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities". It is expected the existing building that will host the TCR (Building 7709) and other existing structures proposed for use may not meet current NPH design requirements. It may not be feasible to upgrade the structures. New SSCs will be designed to perform the intended safety function during and after NPH events (including failure of the structure) and/or equipment and systems will administratively be placed in a safe condition upon notification of severe weather.

Cognizant System Engineer Program

The cognizant system engineer program will be applied to active SC and SS TCR systems. The program is established to appropriately maintain system such that performance of the intended safety function is assured. TCR safety systems are required to perform a safety function for the limited operational duration of the reactor. Therefore, the focus of systems engineering will be on appropriate configuration-managed design, as-built verification, and pre-startup testing.

An alternative methodology is proposed for development of the TCR DSA. The methodology in NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors", is proposed as the alternative methodology. TSRs will be derived in the DSA and documented consistent with DOE G 423.1-1B, "Implementation Guide for Use in Developing Technical Safety Requirements"[17].

The TCR program is in the process of developing a preliminary COR for the design, construction, and operation of the TCR.

7. HAZARD IDENTIFICATION

Consistent with 10 CFR 830 and DOE-STD-1027, the TCR is preliminarily categorized as Nuclear Hazard Category 2. The TCR is a Category B reactor as defined in the Standard. The TCR core contains greater than a safe fissile mass of U-235. Based on pre- and post-irradiation analysis of the core, it is expected the radiological inventory Category 2 TQ sum of ratios may also be greater than unity. The current upper bound on uranium fuel (either UO_2, UC, UN, or mixture thereof) is 250 kg total U.

No formal hazard identification has been performed; however, the hazards inherent in the operation of nuclear reactors are well known. The primary hazard is overheating of the fuel due to various initiating events causing the loss of containment for the fuel (i.e., cladding, reactor vessel, coolant system, and confinement system) and release of fission products. Nuclear criticality hazards during core handling activities are anticipated. Although the presence of a high-pressure gas system is typically considered a standard industrial hazard (SIH) or a potential accident initiator, the reactor is proposed to be equipped with a high-pressure primary gas coolant loop which could also represent a non SIH.

8. KEY SAFETY DECISIONS

Design decisions related to reactor and core design could have cost/schedule impacts and could influence key safety decisions. A primary design decision is reactor power and operational duration. Higher reactor power levels and a longer period of operation result in a larger fission product inventory. These decisions affect the source term and consequence evaluation and could result in the specification of additional controls. Specifically, it is likely a confinement and ventilation system will be required to mitigate a postulated fission product release.

The SDS approach and scoping calculations performed to-date consider bounding cases, and no non-conservatisms have been identified. By considering a conservative safety envelope, it is unlikely safety decisions encountered as the design matures would have unexpected negative impacts on program cost or schedule.

9. RISKS AND OPPORTUNITIES – PROJECT SAFETY DECISIONS

There are several program level risks/decisions that could significantly affect the program and/or major safety strategy decisions. For example, sourcing HALEU could present a program cost/schedule risk. Such risks will be managed in accordance with the program risk management plan. There are risks associated with the novel approach to design, manufacturing, and qualification of advanced manufactured components. Typical reactor safety strategy places significant credit on fuel cladding confinement function (i.e., the first containment barrier). As discussed previously, it is an initial condition the QA plan will assure equipment/items, whether procured or manufactured, are capable of performing intended safety functions.

Based on the Technologies or Initiators listed in DOE-STD-1189, Table C-1, “Sample Considerations for Risk and Opportunity Analysis”, several items appear most applicable to TCR program design and manufacturing platforms. It is possible programmatic risks and opportunities could impact the safety design basis; however, the base technology associated with the safety design basis is not anticipated to be unique. Mitigation strategies for challenges associated with novel design and manufacturing techniques are primary objectives of the TCR program. Consequently, resultant safety strategy decisions to address programmatic risks will likely necessitate increased rigor in QA, increased reliance on other/additional conventional controls and/or justification via reduced risk inherent in small reactors and short operational duration.

10. SAFETY ANALYSIS APPROACH AND PLAN

The safety analysis approach and plan for the TCR presents a unique challenge. DOE is the regulatory authority and has standards and guidance for the development of safety basis documents for categorized nuclear facilities. The standards and guidance are not, however, well suited for nuclear reactor facilities. 10 CFR 830 provides a DSA safe-harbor methodology for DOE reactors in NRC Regulatory Guide 1.70, “Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants”[18]. This NRC guidance is specific to light water power reactors. DOE acknowledges in DOE G 421.1-2A, that NUREG-1537 (the TCR proposed alternative DSA methodology) provides relevant guidance for nonpower reactors but leaves out elements that should be included. Specifically, for DOE nuclear reactors, hazard analysis and categorization of the facility and applicable facility codes and standards should be included. In addition, DOE O 5480.30, “Nuclear Reactor Safety Design Criteria”[19], contains requirements that all DOE reactor designs be evaluated and compared with the design criteria in the Order and the results included in the DSA.

The challenge for the TCR safety analysis is to implement a framework integrating NUREG-1537 and other relevant standards and guidance whose complexity is commensurate with the hazard of the facility. As previously discussed, a graded approach to the safety analysis is proposed based on short operational duration and concomitant low fuel burnup. While the TCR is not an enduring facility and the fuel burnup (i.e., fission product inventory) is comparatively small to a typical DOE reactor, a bounding unmitigated consequence at the site boundary has the potential to exceed the EG. Therefore, the following discussion is provided to describe and derive the graded-approach for the safety analysis

As a starting point, NUREG-1537, Chapter 13 is titled “Accident Analysis”, and key points of guidance focus on characterizing accidents falling into reactor-specific categories as follows:

- Insertion of excess reactivity
- Loss of coolant
- Loss of coolant flow
- Mishandling/malfunction of fuel
- Experiment malfunction (not applicable to TCR)
- Loss of normal electrical power
- External events
- Mishandling/malfunction of equipment

In addition to the above categories, NUREG-1537 specifies the designation of an MHA. The MHA is a postulated fission product release with radiological consequences that exceed all other accidents considered credible. The MHA could be any of the following:

- A specified fraction of fuel in the core melts.
- Cladding is stripped from a specified fraction of the core fuel plates or elements.
- Fuel encapsulation bursts, releasing gaseous fission products to the pool (not applicable to the TCR) or the air.
- A fueled experiment melts or fails catastrophically in the pool or in the air.

NUREG-1537 recommends hazard scenarios in each category be systematically evaluated to identify the most limiting accident for detailed quantitative analysis; it does not specify a method or process for identifying, characterizing, or analyzing credible hazard scenarios. Current DOE and NRC licensing guidance provides for a risk-informed and/or performance-based approach to hazard scenario characterization. NUREG-1537 does not reference or require the implementation of any specific NRC safety analysis framework/methods.

A principle element of new NRC licensing initiatives is the evaluation of hazard scenarios via explicit quantification of probabilistic risk (i.e., probabilistic risk assessment) and resultant consequence. Guidelines/methods for hazards analysis and accident analysis for DOE facilities/activities, such as DOE-STD-3009, allows for a more qualitative (or semi-quantitative) approach. DOE-STD-3009 establishes qualitative consequence thresholds and event likelihood and risk ranking bins (shown in Table 10-1, Table 10-2, and Table 10-3, respectively) for use in characterizing hazard and accident scenarios.

Table 10-1. Consequence Thresholds

Consequence Level	Off-site	Collocated Worker
High	≥ 25 rem	≥ 100 rem
Moderate	≥ 5 rem	≥ 25 rem
Low	< 5 rem	< 25 rem

Table 10-2. Qualitative Likelihood Classification

Frequency	Likelihood Range (/yr)	Definition
Anticipated (A)	$f > 10^{-2}$	Events that may occur several times during the lifetime of the facility.
Unlikely (U)	$10^{-2} > f > 10^{-4}$	Events that are not anticipated to occur during the lifetime of the facility.
Extremely Unlikely (EU)	$10^{-4} > f > 10^{-6}$	Events that will probably not occur during the lifetime of the facility.
Beyond Extremely Unlikely (BEU)	$f < 10^{-6}$	All other accidents.

Table 10-3. Qualitative Risk Bins

		Frequency			
		BEU	**EU**	**U**	**A**
Consequence	**High**	III	II	I	I
	Moderate	IV	III	II	II
	Low	IV	IV	III	III

I = Combination of conclusions from risk analysis that identify situations of major concern
II = Combination of conclusions from risk analysis that identify situations of concern
III = Combination of conclusions from risk analysis that identify situations of minor concern
IV = Combination of conclusions from risk analysis that identify situations of minimal concern

Discretized DOE qualitative risk bins III and IV in Table 10-3 fall completely under the risk divide described in new NRC initiatives and similar evaluation frameworks. Pre-conceptual design evaluations indicate a TCR MHA would likely reside in risk bin III. Therefore, limiting events for the TCR would also fall in DOE risk bins III and IV. This reference point supports a graded approach to the safety analysis. Further, the development of a detailed quantitative assessment of probabilistic risk would offer limited insight for a facility intended to operate for a short period of time.

Therefore, the approach to the TCR safety analysis is proposed to consist of a hazards analysis including hazard categorization and an accident analysis of selected limiting events based on accident consequence and qualitative risk. The accident analysis will include a quantitative evaluation of limiting accident consequences and the selection and functional classification of controls. Accident consequences will be evaluated against DOE thresholds/risk acceptance criteria. The hazards analysis and accident analysis are described further below.

<u>Hazard Analysis</u>

Elements of the proposed hazard analysis process are hazard identification, hazard categorization, and hazard evaluation. Although, the hazard analysis process will be systematic and comprehensive, hazards and process deviations associated with nuclear reactors are well understood. The hazard identification process will develop a bounding inventory for radiological and non-radiological hazards. Given the bounding radiological inventory, final categorization of the facility will be in accordance with DOE-STD-1027.

A graded approach to hazard analysis will be applied. As discussed previously, the short operational duration fundamentally limits hazards associated with the TCR. In addition, the TCR primary and support systems proposed are not complex. Consequently, a largely qualitative hazard analysis approach rather than a probabilistic risk assessment is proposed. As the TCR design enters the conceptual design phase, a multi-disciplinary team of subject matter experts will be established to perform a preliminary hazard analysis at the facility level. The preliminary hazard analysis is expected to be largely expert-based aided by what if type guides. Hazard scenarios will be grouped by categories prescribed by NUREG-1537 and are developed and evaluated to include a brief narrative of the event progression and potential initiators. Based on a comprehensive list of anticipated, available TCR controls, controls are identified that could prevent or mitigate an accident resulting from the scenario.

The hazard and accident analysis will consider the maximally exposed off-site receptor based on recent site-specific meteorology. DOE typically considers the collocated worker to be located at 100 m from the hazard source. For the TCR program, the collocated worker will be considered at either 100 m or 250 m. The 100 m distance is considered for operational events that occur when workers are necessarily present. The 250 m distance is considered for accidents when workers are administratively excluded from the area. Facility worker consequences are qualitatively assessed when workers are necessarily present; otherwise, facility worker consequences are not applicable.

As the design progresses, the hazards analysis will be revised and validated against the design to reflect process level hazards. The output of the hazard analysis will be a listing of credible hazard scenarios applicable to the TCR including a qualitative assessment of consequence and likelihood of occurrence. The qualitative assessment could be based on a set of scoping calculations or a more scenario-specific analysis. For each scenario, a primary preventive and/or mitigative control that stops the accident progression is identified. Secondary controls that could provide additional protection are also listed. Preliminary functional classification of controls is performed to support the design effort. Throughout the hazards analysis process, feedback will be provided to the design through the Safety Design Integration Team (SDIT). When the design is made final, the comprehensive hazards analysis will be finalized and placed under configuration control and the accident analysis will be completed.

Accident Analysis

NUREG-1537 suggests hazard scenarios in each category be systematically evaluated to identify the most limiting accident for detailed quantitative analysis. As previously discussed, qualitative assessment and evaluation of risk will provide the basis for accident selection. These limiting accidents will be termed Design Basis Accidents (DBAs). According to NUREG-1537, the detailed accident analysis for each DBA should provide the following generalized information:

Initial Conditions – Limiting reactor and equipment state including fuel burnup, core configuration.

Initiating Event – Identify causes such as equipment malfunction, operator error. Base the scenario on a single initiating malfunction rather than on multiple causes.

Accident Progression – Assumed equipment operation and malfunction, and operator actions until a final stabilized condition is reached. Discuss functions and actions assumed to occur that change the course of the accident or mitigate the consequences. If credit is taken for mitigation of the accident consequences, discuss the bases used to determine the systems are operable and discuss the system functions.

Systems Damage – Classify damage that might occur to components during the accident until the situation is stabilized. Discuss all components and barriers that could affect the transfer of radiation and radioactivity from the reactor to the public and that ensure continued stability of conditions after the accident.

Analysis – Realistic analyses to demonstrate a detailed, quantitative evaluation of the accident evolution, including the performance of all barriers and the transport of radioactive material. Include assumptions, approximations, methodology, uncertainties, degree of conservatism, margins of safety, and computer codes used.

Source Term – Define and derive the radiation source term.

Radiological Consequence – Evaluate the potential radiological consequences using realistic method. Discuss the degree of conservatism in the evaluation.

In addition to the above characterization of DBAs, controls specifically credited for preventing or mitigating each DBA in the accident analysis will be briefly discussed and described. Depending on the magnitude of the DBA consequence potential, controls will be functionally classified as SC or SS based on the assessed potential consequence. Functional classification of controls will also consider support systems required for the control to perform the safety function. In general, the primary credited control for the first two layers of protection will be functionally classified. Secondary controls considered in each layer will be considered defense-in-depth. It is possible a secondary control for a particular DBA may not require functional classification; however, the same control may be considered a primary control for another DBA and carry a functional classification for that DBA. Administrative controls credited in the accident analysis for preventing or mitigating a DBA are also functionally classified if the safety function rises to the level of SC or SS. An SC or SS administrative control is designated a SAC in accordance with DOE -STD-1186 and will be protected via TSRs.

Safety Analysis Plan

The safety analysis plan proposes to omit elements described in DOE-STD-1189. Table 10-4 lists the key nuclear safety documents proposed for the TCR program.

Table 10-4. DOE-STD-1189 Key Nuclear Safety Documents

Key Nuclear Safety Documents	Proposed for TCR Program
SDS	Yes
R&OA	No
CSDR	No
PDSA	Yes
DSA/TSR	Yes

As discussed in Section 9, technical uncertainty associated with advance manufactured items and fuel technology is understood and could have cost/schedule impacts to the program. Risks and opportunities will be managed at the program level, and safety design implications will be evaluated in updates to the SDS. Program risk management will be practiced consistent with DOE O 413.3B, but it does not require the level of federal oversight as a large DOE capital project.

According to DOE-STD-1189, the primary purpose of the SDS, the Conceptual Design Report, and the Conceptual Safety Design Report (CSDR) is to document the basis for preferred alternatives selection, technology readiness status, assumptions, safety-in-design risks, and opportunities. Although the development of technology related to design and manufacturing is core to the program mission, the base technology (i.e., nuclear fission reactors and associated safety controls) is well understood. Consequently, safety information that might otherwise be documented in a CSDR or Preliminary Safety and Design Results document will be incorporated in revisions to the SDS, Draft PDSA, and PDSA to ensure safety is integrated in the final design. The program submits that robust safety-in-design can be adequately demonstrated and authorized via the proposed nuclear safety documents listed in Table 10-4.

11. SAFETY DESIGN INTEGRATION TEAM – INTERFACE AND INTEGRATION

The TCR program will constitute a multi-disciplinary SDIT to review and oversee the integration of safety in the design process. The SDIT will operate in accordance with a written program, plan, and/or procedure which describes the makeup of the team and how the team functions within the TCR program. During the pre-conceptual and conceptual design stage the SDIT will meet periodically to review and understand the design and to identify potentially unintended consequences of the design decisions. Notwithstanding the effort of the SDIT, safety is core to the design process and is the basis for most of the established design requirements.

As the design matures and moves on to preliminary and final milestones, the SDIT will be informed by a robust design change management system. While all design changes may not require formal briefing and SDIT debate, designs with potential safety design impacts shall be reviewed and consensus reached by the SDIT.

12. REFERENCES

1. DOE-STD-1189-2016, “Integration of Safety into the Design Process,” U.S. Department of Energy, December 2016.
2. DOE O 413.3B, “Program and Project Management for the Acquisition of Capital Assets,” Change 5, U.S. Department of Energy, November 2010.
3. DOE O 420.1C, “Facility Safety,” Change 2, U.S. Department of Energy, July 26, 2018.
4. 10 CFR 830, “Nuclear Safety Management,” Code of Federal Regulations, Office of the Federal Register, January 2001.
5. NRC RG 1.232, “Guidance for Developing Principal Design Criteria for Non-Light-Water Reactors,” U.S. Nuclear Regulatory Commission, April 2018.
6. ASME/NQA-1-2008 with 2009 addendum, “Nuclear Quality Assurance,” American Society of Mechanical Engineers.
7. ASME BPV, Section III, “Piping Design,” American Society of Mechanical Engineers. Current Version.
8. NUREG-1537, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” U.S. Nuclear Regulatory Commission.
9. DOE-STD-3009-2014, “Preparation of Nonreactor Nuclear Facility Documented Safety Analysis,” U.S. Department of Energy, November 2014.
10. FCSE-ISG-14, “Acute Uranium Exposure Standard for Workers,” U.S. Nuclear Regulatory Commission.
11. 10 CFR 50 Appendix A, “General Design Criteria for Nuclear Power Plants,” Code of Federal Regulations, Office of the Federal Register, January 2001.
12. DOE-STD-1027-2018, “Hazard Categorization of DOE Nuclear Facilities,” U.S. Department of Energy, November 2018.
13. DOE G 421.1-2A, “Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830,” U.S. Department of Energy, December 4, 2011.
14. IEEE 379-2014, “IEEE Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems,” Institute of Electrical and Electronics Engineers.
15. IEEE 323-2003 (R2008), “IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers.
16. DOE-STD-1020-2016, “Natural Phenomena Hazards Analysis and Design Criteria for DOE Facilities,” U.S. Department of Energy, December 2016.

17. DOE G 423.1-1B, "Implementation Guide for Use in Developing Technical Safety Requirements" U.S. Department of Energy, March 18, 2011.
18. NRC RG 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants," U.S. Nuclear Regulatory Commission.
19. DOE O 5480.30, "Nuclear Reactor Safety Design Criteria," U.S. Department of Energy, March 2001.

APPENDIX A

DSA Format and Content Summary

Chapter 1 summarizes the principal design bases and considerations, general descriptions of the reactor facility that illustrate the anticipated operations, and the design safety considerations, including the limiting potential accidents. This chapter summarizes the detailed information found in subsequent chapters of the DSA.

Chapter 2 describes the bases for the site selection and describes the applicable site characteristics, including geography, demography, meteorology, hydrology, geology, seismology, and interaction with nearby installations and facilities.

Chapter 3 describes the design bases and facility structures, systems, and components, and the responses to environmental factors on the reactor site (e.g., floods).

Chapter 4 describes the design bases and the functional characteristics of the reactor core and its components. In this chapter, the safety considerations and features of the reactor are discussed.

Chapter 5 lists the design bases and describes the functions of the reactor coolant and associated systems at the facility, including the primary and secondary systems as applicable, and coolant makeup and purification systems. The chapter also describes provisions for adequate heat removal while the reactor is operating and while it is shut down. Note: TCR will have no coolant makeup and purification systems.

Chapter 6 lists the design bases and describes the functions of engineered safety features (ESFs) that may be required to mitigate consequences of postulated accidents at the facility. This includes design-basis accidents and a maximum hypothetical accident (MHA). The MHA, which assumes an incredible failure that can lead to fuel cladding or to a fueled experiment containment breach, is used to bound credible accidents in the accident analysis.

Chapter 7 lists the design bases and describes the functions of the instrumentation and control systems and subsystems at the facility, placing emphasis on safety related systems and safe reactor shutdown.

Chapter 8 lists the design bases and describes the functions of the normal and emergency (if applicable) electrical power systems at the facility.

Chapter 9 lists the design bases and describes the functions of such auxiliary systems at the facility as heating, ventilation, air exhaust, air conditioning, service water, compressed air, and fuel handling and storage.

Chapter 10 lists the design bases and describes the functions of experimental facilities. Non-power reactors are designed with irradiation capabilities for research, education, and technological development. This chapter discusses the characteristics of experiment and irradiation facilities based on the proposed experimental programs. This chapter is not applicable to the TCR since the facility does not contain experimental or irradiation facilities.

Chapter 11 lists the design bases and describes the functions of the radiation protection and the radioactive waste management programs at the facility. This chapter also describes the control of byproduct materials produced in the reactor and utilized under the 10 CFR Part 50 reactor operating license. The description of the radiation protection program should include health physics procedures, monitoring programs for personnel exposures and effluent releases, and assessment and control of radiation doses, both to workers and the public. The program to maintain radiation exposures and releases as low as is reasonably achievable (ALARA) includes the control and disposal of radiological waste from reactor operations and from experimental programs. Note: TCR will not produce any by product materials as a result of its operation.

Chapter 12 lists the bases and describes the functions of plans and procedures for the conduct of facility operations. These include discussions of the management structure, personnel training and evaluation, provisions for safety review and auditing of operations by the safety committees, and other required functions, such as reporting, security planning, emergency planning, and planning for reactor startup.

Chapter 13 lists the bases, scenarios, and analyses of accidents at the reactor facility, and describes an MHA, which may include a fission product release, and radiological consequences to the operational staff reactor users, the public, and the environment. The function of ESFs is discussed in the accident analysis, as applicable. Note: TCR will not host a user facility therefore only operational staff and public/environmental consequences will be addressed.

Chapter 14 presents the technical specifications, which state the operating limits and conditions and other requirements for the facility to acceptably ensure protection of the health and safety of the public. Note: A separate Technical Safety Requirements document will be generated in compliance with 10 CFR 830.205, Subpart B, Safety Basis Requirements.

Chapter 15 concerns financial qualifications of the non-power reactor applicant for initial construction, continuing operations, and decommissioning. Note: The TCR is government-funded therefore financial considerations are not applicable.

Chapter 16 discusses assembling the reactor core on-site in preparation for operation.

Chapter 17 addresses on-site activities associated with disassembling the core upon completion of operation and evaluation/analysis of the core while on the TCR site. This chapter also gives guidance on decommissioning.

Chapter 18 discusses the conversion of the reactor from highly enriched uranium (HEU) fuel to low-enriched uranium (LEU) fuel, includes topics covered in Chapters 1 to 17 as related to HEU to LEU conversions. Note: TCR will utilize high-enriched LEU fuel so this chapter is not applicable.

APPENDIX B

Example Preliminary TCR Principal Design Criteria

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
mHTGR-1	*Quality standards and records* Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.	TCR-1	*Quality standards and records* Structures, systems, and components important to safety shall be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. A quality assurance program shall be established and implemented in order to provide adequate assurance that these structures, systems, and components will satisfactorily perform their safety functions. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components important to safety shall be maintained by or under the control of the nuclear power unit licensee throughout the life of the unit.	No differences between RG 1.232 and TCR.
mHTGR-2	*Design bases for protection against natural phenomena.* Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed.	TCR-2	*Design bases for protection against natural phenomena.* Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed.	See Note 1.

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
mHTGR-3	*Fire protection.* Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and fire- resistant materials shall be used wherever practical throughout the unit, particularly in locations with structures, systems, or components important to safety. Fire detection and fighting systems of appropriate capacity and capability shall be provided and designed to minimize the adverse effects of fires on structures, systems, and components important to safety. Firefighting systems shall be designed to ensure that their rupture or inadvertent operation does not significantly impair the safety capability of these structures, systems, and components.	TCR-3	*Fire protection.* Structures, systems, and components important to safety shall be designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions. Noncombustible and fire- resistant materials shall be used wherever practical throughout the unit, particularly in locations with structures, systems, or components important to safety. Fire detection and fighting systems of appropriate capacity and capability shall be provided and designed to minimize the adverse effects of fires on structures, systems, and components important to safety. Firefighting systems shall be designed to ensure that their rupture or inadvertent operation does not significantly impair the safety capability of these structures, systems, and components.	See Note 2.
mHTGR-4	*Environmental and dynamic effects design bases.* Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents. These structures, systems, and components shall be appropriately protected against dynamic effects, including the effects of missiles originating both inside and outside the reactor helium pressure boundary, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. However, dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping.	N/A	Not applicable to TCR due the extremely low probability of fluid system pipe rupture during the design life of the reactor. Design basis events involving dynamic effects can be safely excluded.	N/A
mHTGR-5	*Sharing of structures, systems, and components.* Structures, systems, and components important to safety shall not be shared among nuclear power units unless it can be shown that such sharing will not significantly impair their ability to perform their safety functions, including, in the event of an accident in one unit, an orderly shutdown and cooldown of the remaining units.	N/A	Not applicable due to only one anticipated TCR unit.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
ARDC-10	*Reactor design.* The reactor core and associated coolant, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.	TCR-4	*Reactor design.* The reactor system and associated heat removal, control, and protection systems shall be designed with appropriate margin to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.	See Note 3.
mHTGR-11	*Reactor inherent protection.* The reactor core and associated systems that contribute to reactivity feedback shall be designed so that, in the power operating range, the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity.	TCR-5	*Reactor inherent protection.* The reactor core and associated systems that contribute to reactivity feedback shall be designed so that, in the power operating range, the net effect of the prompt inherent nuclear feedback characteristics tends to compensate for a rapid increase in reactivity.	No differences between RG 1.232 and TCR.
mHTGR-12	*Suppression of reactor power oscillations.* The reactor core; associated structures; and associated coolant, control, and protection systems shall be designed to ensure that power oscillations that can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.	TCR-6	*Suppression of reactor power oscillations.* The reactor core and associated control and protection systems shall be designed to ensure that power oscillations that can result in conditions exceeding specified acceptable fuel design limits are not possible or can be reliably and readily detected and suppressed.	See Note 4.
mHTGR-13	*Instrumentation and control.* Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions, as appropriate, to ensure adequate safety, including those variables and systems that can affect the fission process and the integrity of the reactor core, reactor helium pressure boundary, and functional containment. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.	TCR-7	*Instrumentation and control.* Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions, as appropriate, to ensure adequate safety, including those variables and systems that can affect the fission process and the integrity of the reactor core, reactor helium pressure boundary, and functional containment. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.	No differences between RG 1.232 and TCR.
mHTGR-14	*Reactor helium pressure boundary.* The reactor helium pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, of gross rupture, and of unacceptable ingress of moisture, air, secondary coolant, or other fluids.	TCR-8	*Reactor helium pressure boundary.* The reactor helium pressure boundary shall be designed, fabricated, erected, and tested so as to have an extremely low probability of abnormal leakage, of rapidly propagating failure, of gross rupture, and of unacceptable ingress of moisture, air, secondary coolant, or other fluids.	No differences between RG 1.232 and TCR.

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
mHTGR-15	*Reactor helium pressure boundary design.* All systems that are part of the reactor helium pressure boundary, such as the reactor system, vessel system, and heat removal systems, and the associated auxiliary, control, and protection systems, shall be designed with sufficient margin to ensure that the design conditions of the reactor helium pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.	TCR-9	*Reactor helium pressure boundary design.* All systems that are part of the reactor helium pressure boundary, such as the reactor system, vessel system, and heat removal systems, and the associated auxiliary, control, and protection systems, shall be designed with sufficient margin to ensure that the design conditions of the reactor helium pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.	No differences between RG 1.232 and TCR.
mHTGR-16	*Containment and design.* A reactor functional containment, consisting of multiple barriers internal and/or external to the reactor and its cooling system, shall be provided to control the release of radioactivity to the environment and to ensure that the functional containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.	TCR-10	*Containment and design.* A reactor functional containment, consisting of multiple barriers internal and/or external to the reactor and its cooling system, shall be provided to control the release of radioactivity to the environment and to ensure that the functional containment design conditions important to safety are not exceeded for as long as postulated accident conditions require.	No differences between RG 1.232 and TCR.
ARDC-17	*Electric power systems.* Electric power systems shall be provided when required to permit functioning of structures, systems, and components. The safety function for each power system shall be to provide sufficient capacity and capability to ensure that (1) that the design limits for the fission product barriers are not exceeded as a result of anticipated operational occurrences and (2) safety functions that rely on electric power are maintained in the event of postulated accidents. The electric power systems shall include an onsite power system and an additional power system. The onsite electric power system shall have sufficient independence, redundancy, and testability to perform its safety functions, assuming a single failure. An additional power system shall have sufficient independence and testability to perform its safety function. If electric power is not needed for anticipated operational occurrences or postulated accidents, the design shall demonstrate that power for important to safety functions is provided.	TCR-11	*Electric power systems.* Electric power systems shall be provided when required to permit functioning of structures, systems, and components. The safety function for each power system shall be to provide sufficient capacity and capability to ensure that (1) that the design limits for the fission product barriers are not exceeded as a result of anticipated operational occurrences and (2) safety functions that rely on electric power are maintained in the event of postulated accidents. The electric power systems shall include an onsite power system and an additional power system. The onsite electric power system shall have sufficient independence, redundancy, and testability to perform its safety functions, assuming a single failure. An additional power system shall have sufficient independence and testability to perform its safety function. If electric power is not needed for anticipated operational occurrences or postulated accidents, the design shall demonstrate that power for important to safety functions is provided.	See Note 3.

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
mHTGR-18	*Inspection and testing of electric power systems.* Electric power systems important to safety shall be designed to permit appropriate periodic inspection and testing of important areas and features, such as wiring, insulation, connections, and switchboards, to assess the continuity of the systems and the condition of their components. The systems shall be designed with a capability to test periodically (1) the operability and functional performance of the components of the systems, such as onsite power sources, relays, switches, and buses, and (2) the operability of the systems as a whole and, under conditions as close to design as practical, the full operation sequence that brings the systems into operation, including operation of applicable portions of the protection system, and the transfer of power among systems.	N/A	Not applicable due to the brief design life of the reactor.	N/A
mHTGR-19	*Control room.* A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem total effective dose equivalent as defined in § 50.2 for the duration of the accident. Adequate habitability measures shall be provided to permit access and occupancy of the control room during normal operations and under accident conditions. Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.	TCR-12	*Control room.* A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Adequate radiation protection shall be provided to permit access and occupancy of the control room under accident conditions without personnel receiving radiation exposures in excess of 5 rem total effective dose equivalent as defined in § 50.2 for the duration of the accident. Adequate habitability measures shall be provided to permit access and occupancy of the control room during normal operations and under accident conditions. Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.	No differences between RG 1.232 and TCR.

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
ARDC-20	*Protection system functions.* The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety.	TCR-13	*Protection system functions and reliability.* The protection system shall be designed (1) to initiate automatically the operation of appropriate systems including the reactivity control systems, to assure that specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of systems and components important to safety. Additionally, redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated.	Combined ARDC-20 and reliability portions from ARDC-21.
ARDC-21	*Protection system reliability and testability.* protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. The protection system shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.	N/A	Protection system testability is not applicable to the TCR due to its brief deign life. Reliability is applicable and has been added to TCR-13.	N/A
mHTGR-22	*Protection system independence.* The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.	TCR-14	*Protection system independence.* The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.	No differences between RG 1.232 and TCR.

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
mHTGR-23	*Protection system failure modes.* The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.	TCR-15	*Protection system failure modes.* The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced.	No differences between RG 1.232 and TCR.
mHTGR-24	*Separation of protection and control systems.* The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.	TCR-16	*Separation of protection and control systems.* The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.	No differences between RG 1.232 and TCR.
ARDC-25	*Protection system requirements for reactivity control malfunctions.* The protection system shall be designed to ensure that specified acceptable fuel design limits are not exceeded during any anticipated operational occurrence accounting for a single malfunction of the reactivity control systems.	TCR-17	*Protection system requirements for reactivity control malfunctions.* The protection system shall be designed to ensure that specified acceptable fuel design limits are not exceeded during any anticipated operational occurrence accounting for a single malfunction of the reactivity control systems.	No differences between RG 1.232 and TCR.

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
ARDC-26	*Reactivity control systems.* A minimum of two reactivity control systems or means shall provide: (1) A means of inserting negative reactivity at a sufficient rate and amount to assure, with appropriate margin for malfunctions, that the design limits for the fission product barriers are not exceeded and safe shutdown is achieved and maintained during normal operation, including anticipated operational occurrences. (2) A means which is independent and diverse from the other(s), shall be capable of controlling the rate of reactivity changes resulting from planned, normal power changes to assure that the design limits for the fission product barriers are not exceeded. (3) A means of shutting down the reactor and maintaining, at a minimum, a safe shutdown condition following a postulated accident, with appropriate margin for malfunctions, shall be provided. A means for holding the reactor shutdown under conditions which allow for interventions such as fuel loading, inspection and repair shall be provided.	TCR-18	*Reactivity control systems.* A minimum of two reactivity control systems or means shall provide: (1) A means of inserting negative reactivity at a sufficient rate and amount to assure, with appropriate margin for malfunctions, that the design limits for the fission product barriers are not exceeded and safe shutdown is achieved and maintained during normal operation, including anticipated operational occurrences. (2) A means which is independent and diverse from the other(s), shall be capable of controlling the rate of reactivity changes resulting from planned, normal power changes to assure that the design limits for the fission product barriers are not exceeded. (3) A means of shutting down the reactor and maintaining, at a minimum, a safe shutdown condition following a postulated accident, with appropriate margin for malfunctions, shall be provided. A means for holding the reactor shutdown under conditions which allow for interventions such as fuel loading, inspection and repair shall be provided.	No differences between RG 1.232 and TCR.
mHTGR-22	*Reactivity limits.* The reactor core, including the reactivity control systems, shall be designed with appropriate limits on the potential amount and rate of reactivity increase to ensure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor helium pressure boundary greater than limited local yielding, nor (2) sufficiently disturb the core, its support structures, or other reactor vessel internals to impair significantly the capability to cool the core.	TCR-19	*Reactivity limits.* The reactor core, including the reactivity control systems, shall be designed with appropriate limits on the potential amount and rate of reactivity increase to ensure that the effects of postulated reactivity accidents can neither (1) result in damage to the reactor helium pressure boundary greater than limited local yielding, nor (2) sufficiently disturb the core, its support structures, or other reactor vessel internals to impair significantly the capability to cool the core.	No differences between RG 1.232 and TCR.

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
mHTGR-23	*Protection against anticipated operational occurrences.* The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	TCR-20	*Protection against anticipated operational occurrences.* The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences.	No differences between RG 1.232 and TCR.
mHTGR-24	*Quality of reactor helium pressure boundary.* Components that are part of the reactor helium pressure boundary shall be designed, fabricated, erected, and tested to the highest quality standards practical. Means shall be provided for detecting and, to the extent practical, identifying the location of the source of reactor helium leakage. Means shall be provided for detecting ingress of moisture, air, secondary coolant, or other fluids to within the reactor helium pressure boundary.	TCR-21	*Quality of reactor helium pressure boundary.* Components that are part of the reactor helium pressure boundary shall be designed, fabricated, erected, and tested to the highest quality standards practical. Means shall be provided for detecting and, to the extent practical, identifying the location of the source of reactor helium leakage. Means shall be provided for detecting ingress of moisture, air, secondary coolant, or other fluids to within the reactor helium pressure boundary.	No differences between RG 1.232 and TCR.
ARDC-25	*Fracture prevention of reactor helium pressure boundary.* The reactor helium pressure boundary shall be designed with sufficient margin to ensure that, when stressed under operating, maintenance, testing, and postulated accident conditions, (1) the boundary behaves in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures, service degradation of material properties, creep, fatigue, stress rupture, and other conditions of the boundary material under operating, maintenance, testing, and postulated accident conditions and the uncertainties in determining (1) material properties, (2) the effects of irradiation and helium composition, including contaminants and reaction products, on material properties, (3) residual, steady-state, and transient stresses, and (4) size of flaws.	TCR-22	*Fracture prevention of reactor helium pressure boundary.* The reactor helium pressure boundary shall be designed with sufficient margin to ensure that, when stressed under operating, maintenance, testing, and postulated accident conditions, (1) the boundary behaves in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures, service degradation of material properties, creep, fatigue, stress rupture, and other conditions of the boundary material under operating, maintenance, testing, and postulated accident conditions and the uncertainties in determining (1) material properties, (2) the effects of irradiation and helium composition, including contaminants and reaction products, on material properties, (3) residual, steady-state, and transient stresses, and (4) size of flaws.	No differences between RG 1.232 and TCR.
mHTGR-32	*Inspection of reactor helium pressure boundary.* Components that are part of the reactor helium pressure boundary shall be designed to permit (1) periodic inspection and functional testing of important areas and features to assess their structural and leaktight integrity, and (2) an appropriate material surveillance program for the reactor vessel.	N/A	Inspection and testing of components is not applicable to the TCR due to its brief deign life.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
ARDC-33	*Reactor coolant inventory maintenance.* A system to maintain reactor coolant inventory for protection against small breaks in the reactor coolant boundary shall be provided as necessary to ensure that specified acceptable fuel design limits are not exceeded as a result of reactor coolant inventory loss due to leakage from the reactor coolant boundary and rupture of small piping or other small components that are part of the boundary. The system shall be designed to ensure that the system safety function can be accomplished using the piping, pumps, and valves used to maintain reactor coolant inventory during normal reactor operation.	N/A	Like the mHTGR, the TCR uses helium as a coolant and is not dependent on maintaining "inventory" for sufficient core heat removal.	N/A
ARDC-34	*Residual heat removal.* A system to remove residual heat shall be provided. For normal operations and anticipated operational occurrences, the system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant boundary are not exceeded. Suitable redundancy in components and features and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that the system safety function can be accomplished, assuming a single failure.	TCR-23	*Residual heat removal.* A system to remove residual heat shall be provided. For normal operations and anticipated operational occurrences, the system safety function shall be to transfer fission product decay heat and other residual heat from the reactor core at a rate such that specified acceptable fuel design limits and the design conditions of the reactor coolant boundary are not exceeded. During postulated accidents, the system safety functions shall provide effective cooling. Suitable redundancy in components and features and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that the system safety function can be accomplished, assuming a single failure.	See Note 5.
ARDC-35	*Emergency core cooling system.* A system to assure sufficient core cooling during postulated accidents and to remove residual heat following postulated accidents shall be provided. The system safety function shall be to transfer heat from the reactor core during and following postulated accidents such that fuel and clad damage that could interfere with continued effective core cooling is prevented.	N/A	Like mHTGRs, maintaining the helium inventory is not necessary for the TCR to maintain effective cooling. Requirements for cooling during postulated accidents have been add to TCR-24.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
ARDC-36	*Inspection of emergency core cooling system.* A system that provides emergency core cooling shall be designed to permit appropriate periodic inspection of important components to ensure the integrity and capability of the system.	N/A	Inspection of components is not applicable to the TCR due to its brief deign life.	N/A
ARDC-37	*Testing of emergency core cooling system.* A system that provides emergency core cooling shall be designed to permit appropriate periodic functional testing to ensure (1) the structural and leaktight integrity of its components, (2) the operability and performance of the system components, and (3) the operability of the system as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the system into operation, including operation of any associated systems and interfaces necessary to transfer decay heat to the ultimate heat sink.	N/A	Inspection and testing of components is not applicable to the TCR due to its brief deign life.	N/A
ARDC-38	*Containment heat removal.* A system to remove heat from the reactor containment shall be provided as necessary to maintain the containment pressure and temperature within acceptable limits following postulated accidents. Suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities shall be provided to ensure that the system safety function can be accomplished, assuming a single failure.	N/A	Like the mHTGR, a functional containment or confinement approach is followed for radionuclide retention. Containment heat removal is not applicable for the TCR.	N/A
ARDC-39	*Inspection of containment heat removal system.* The containment heat removal system shall be designed to permit appropriate periodic inspection of important components to ensure the integrity and capability of the system.	N/A	Inspection and testing of components is not applicable to the TCR due to its brief deign life.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	Title & Content	DC#	Title & Content, with Highlighted Differences in Red	
ARDC-40	*Testing of containment heat removal system.* The containment heat removal system shall be designed to permit appropriate periodic functional testing to ensure (1) the structural and leaktight integrity of its components, (2) the operability and performance of the system components, and (3) the operability of the system as a whole, and under conditions as close to the design as practical, the performance of the full operational sequence that brings the system into operation, including the operation of associated systems.	N/A	Containment heat removal is not applicable for the TCR.	N/A
ARDC-41	*Containment atmosphere cleanup.* Systems to control fission products and other substances that may be released into the reactor containment shall be provided as necessary to reduce, consistent with the functioning of other associated systems, the concentration and quality of fission products released to the environment following postulated accidents and to control the concentration of other substances in the containment atmosphere following postulated accidents to ensure that containment integrity and other safety functions are maintained. Each system shall have suitable redundancy in components and features and suitable interconnections, leak detection, isolation, and containment capabilities to ensure that its safety function can be accomplished, assuming a single failure.	N/A	Containment heat removal is not applicable for the TCR.	N/A
ARDC-42	*Inspection of containment atmosphere cleanup systems.* The containment atmosphere cleanup systems shall be designed to permit appropriate periodic inspection of important components, such as filter frames, ducts, and piping to assure the integrity and capability of the systems.	N/A	Inspection and testing of components is not applicable to the TCR due to its brief deign life.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
ARDC-43	*Testing of containment atmosphere cleanup systems.* The containment atmosphere cleanup systems shall be designed to permit appropriate periodic functional testing to ensure (1) the structural and leaktight integrity of its components, (2) the operability and performance of the system components, and (3) the operability of the systems as a whole and, under conditions as close to design as practical, the performance of the full operational sequence that brings the systems into operation, including the operation of associated systems.	N/A	Inspection and testing of components is not applicable to the TCR due to its brief deign life.	N/A
ARDC-44	*Structural and equipment cooling.* A system to transfer heat from structures, systems, and components important to safety to an ultimate heat sink shall be provided, as necessary, to transfer the combined heat load of these structures, systems, and components under normal operating and accident conditions. Suitable redundancy in components and features and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that the system safety function can be accomplished, assuming a single failure.	TCR-24	*Structural and equipment cooling.* A system to transfer heat from structures, systems, and components important to safety to an ultimate heat sink shall be provided, as necessary, to transfer the combined heat load of these structures, systems, and components under normal operating and accident conditions. Suitable redundancy in components and features and suitable interconnections, leak detection, and isolation capabilities shall be provided to ensure that the system safety function can be accomplished, assuming a single failure.	No differences between RG 1.232 and TCR.
ARDC-45	*Inspection of structural and equipment cooling systems.* The structural and equipment cooling systems shall be designed to permit appropriate periodic inspection of important components, such as heat exchangers and piping, to ensure the integrity and capability of the systems.	N/A	Inspection and testing of components is not applicable to the TCR due to its brief design life.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
ARDC-46	*Testing of structural and equipment cooling systems.* The structural and equipment cooling systems shall be designed to permit appropriate periodic functional testing to ensure (1) the structural and leaktight integrity of their components, (2) the operability and performance of the system components, and (3) the operability of the systems as a whole and, under conditions as close to design as practical, the performance of the full operational sequences that bring the systems into operation for reactor shutdown and postulated accidents, including the operation of associated systems.	N/A	Inspection and testing of components is not applicable to the TCR due to its brief deign life.	N/A
ARDC-50	*Containment design basis.* The containment structure, including access openings, penetrations, and the containment heat removal system shall be designed so that the containment structure and its internal compartments can accommodate, without exceeding the design leakage rate and with sufficient margin, the calculated pressure and temperature conditions resulting from postulated accidents. This margin shall reflect consideration of (1) the effects of potential energy sources that have not been included in the determination of the peak conditions, (2) the limited experience and experimental data available for defining accident phenomena and containment responses, and (3) the conservatism of the calculational model and input parameters.	N/A	Like the mHTGR, a functional containment or confinement approach is followed for radionuclide retention. A low leakage, traditional containment design is not applicable for the TCR.	N/A
ARDC-51	*Fracture prevention of containment pressure boundary.* The boundary of the containment structure shall be designed with sufficient margin to ensure that, under operating, maintenance, testing, and postulated accident conditions, (1) its materials behave in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the containment boundary materials during operation, maintenance, testing, and postulated accident conditions, and the uncertainties in determining (1) material properties, (2) residual, steady-state, and transient stresses, and (3) size of flaws.	N/A	A low leakage, traditional containment design is not applicable for the TCR.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		**TCR**		**Notes & Rationale**
DC#	**Title & Content**	**DC#**	**Title & Content**, with Highlighted Differences in Red	
ARDC-52	*Capability for containment leakage rate testing.* The containment structure and other equipment that may be subjected to containment test conditions shall be designed so that periodic integrated leakage rate testing can be conducted at containment design pressure.	N/A	A low leakage, traditional containment design is not applicable for the TCR.	N/A
ARDC-53	*Provisions for containment testing and inspection.* The containment structure shall be designed to permit (1) appropriate periodic inspection of all important areas, such as penetrations, (2) an appropriate surveillance program, and (3) periodic testing at containment design pressure of the leaktightness of penetrations that have resilient seals and expansion bellows.	N/A	Inspection and testing of components is not applicable to the TCR due to its brief deign life.	N/A
ARDC-54	*Piping systems penetrating containment.* Piping systems penetrating the containment structure shall be provided with leak detection, isolation, and containment capabilities having redundancy, reliability, and performance capabilities that reflect the importance to safety of isolating these piping systems. Such piping systems shall be designed with the capability to verify, by testing, the operational readiness of any isolation valves and associated apparatus periodically and to confirm that valve leakage is within acceptable limits.	N/A	A low leakage, traditional containment design is not applicable for the TCR.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
ARDC-55	*Reactor coolant boundary penetrating containment.* Each line that is part of the reactor coolant boundary and that penetrates the containment structure shall be provided with containment isolation valves, as follows, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis: (1) One locked closed isolation valve inside and one locked closed isolation valve outside containment; or (2) One automatic isolation valve inside and one locked closed isolation valve outside containment; or (3) One locked closed isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment; or (4) One automatic isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment. Isolation valves outside containment shall be located as close to containment as practical and upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety. Other appropriate requirements to minimize the probability or consequences of an accidental rupture of these lines or of lines connected to them shall be provided as necessary to ensure adequate safety. Determination of the appropriateness of these requirements, such as higher quality in design, fabrication, and testing; additional provisions for inservice inspection; protection against more severe natural phenomena; and additional isolation valves and containment, shall include consideration of the population density, use characteristics, and physical characteristics of the site environs.	N/A	A low leakage, traditional containment design is not applicable for the TCR.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
ARDC-56	*Containment isolation.* Each line that connects directly to the containment atmosphere and penetrates the containment structure shall be provided with containment isolation valves as follows, unless it can be demonstrated that the containment isolation provisions for a specific class of lines, such as instrument lines, are acceptable on some other defined basis: (1) One locked closed isolation valve inside and one locked closed isolation valve outside containment; or (2) One automatic isolation valve inside and one locked closed isolation valve outside containment; or (3) One locked closed isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment; or (4) One automatic isolation valve inside and one automatic isolation valve outside containment. A simple check valve may not be used as the automatic isolation valve outside containment. Isolation valves outside containment shall be located as close to the containment as practical and upon loss of actuating power, automatic isolation valves shall be designed to take the position that provides greater safety.	N/A	A low leakage, traditional containment design is not applicable for the TCR.	N/A
ARDC-57	*Closed system isolation valves.* Each line that penetrates the containment structure and is neither part of the reactor coolant boundary nor connected directly to the containment atmosphere shall have at least one containment isolation valve, unless it can be demonstrated that the containment safety function can be met without an isolation valve and assuming failure of a single active component. The isolation valve, if required, shall be either automatic, or locked closed, or capable of remote manual operation. This valve shall be outside containment and located as close to the containment as practical. A simple check valve may not be used as the automatic isolation valve.	N/A	A low leakage, traditional containment design is not applicable for the TCR.	N/A

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		TCR		Notes & Rationale
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
mHTGR-60	*Control of releases of radioactive materials to the environment.* The nuclear power unit design shall include means to control suitably the release of radioactive materials in gaseous and liquid effluents and to handle radioactive solid wastes produced during normal reactor operation, including anticipated operational occurrences. Sufficient holdup capacity shall be provided for retention of gaseous and liquid effluents containing radioactive materials, particularly where unfavorable site environmental conditions can be expected to impose unusual operational limitations upon the release of such effluents to the environment.	TCR-25	*Control of releases of radioactive materials to the environment.* The nuclear power unit design shall include means to control suitably the release of radioactive materials in gaseous and liquid effluents and to handle radioactive solid wastes produced during normal reactor operation, including anticipated operational occurrences. Sufficient holdup capacity shall be provided for retention of gaseous and liquid effluents containing radioactive materials, particularly where unfavorable site environmental conditions can be expected to impose unusual operational limitations upon the release of such effluents to the environment.	No differences, See Note 6.
mHTGR-61	*Fuel storage and handling and radioactivity control.* The fuel storage and handling, radioactive waste, and other systems that may contain radioactivity shall be designed to ensure adequate safety under normal and postulated accident conditions. These systems shall be designed (1) with a capability to permit appropriate periodic inspection and testing of components important to safety, (2) with suitable shielding for radiation protection, (3) with appropriate containment, confinement, and filtering systems, (4) with a residual heat removal capability having reliability and testability that reflects the importance to safety of decay heat and other residual heat removal, and (5) to prevent significant reduction in fuel storage cooling under accident conditions.	TCR-26	*Fuel storage and handling and radioactivity control.* The fuel storage and handling, radioactive waste, and other systems that may contain radioactivity shall be designed to ensure adequate safety under normal and postulated accident conditions. These systems shall be designed (1) with a capability to permit appropriate periodic inspection and testing of components important to safety, (2) with suitable shielding for radiation protection, (3) with appropriate containment, confinement, and filtering systems, (4) with a residual heat removal capability having reliability and testability that reflects the importance to safety of decay heat and other residual heat removal, and (5) to prevent significant reduction in fuel storage cooling under accident conditions.	No differences, See Note 6.
mHTGR-62	*Prevention of criticality in fuel storage and handling.* Criticality in the fuel storage and handling system shall be prevented by physical systems or processes, preferably by use of geometrically safe configurations.	TCR-27	*Prevention of criticality in fuel storage and handling.* Criticality in the fuel storage and handling system shall be prevented by physical systems or processes, preferably by use of geometrically safe configurations.	No differences between RG 1.232 and TCR.
mHTGR-63	*Monitoring fuel and waste storage.* Appropriate systems shall be provided in fuel storage and radioactive waste systems and associated handling areas (1) to detect conditions that may result in loss of residual heat removal capability and excessive radiation levels and (2) to initiate appropriate safety actions.	TCR-28	*Monitoring fuel and waste storage.* Appropriate systems shall be provided in fuel storage and radioactive waste systems and associated handling areas (1) to detect conditions that may result in loss of residual heat removal capability and excessive radiation levels and (2) to initiate appropriate safety actions.	No differences, See Note 6.

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		**TCR**		**Notes & Rationale**
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
mHTGR-64	*Monitoring radioactivity releases.* Means shall be provided for monitoring the reactor building atmosphere, effluent discharge paths, and plant environs for radioactivity that may be released from normal operations, including anticipated operational occurrences, and from postulated accidents.	TCR-29	*Monitoring radioactivity releases* Means shall be provided for monitoring the reactor building atmosphere, effluent discharge paths, and plant environs for radioactivity that may be released from normal operations, including anticipated operational occurrences, and from postulated accidents.	No differences between RG 1.232 and TCR.
mHTGR-70	*Reactor vessel and reactor system structural design basis.* The design of the reactor vessel and reactor system shall be such that their integrity is maintained during postulated accidents (1) to ensure the geometry for passive removal of residual heat from the reactor core to the ultimate heat sink and (2) to permit sufficient insertion of the neutron absorbers to provide for reactor shutdown.	N/A	If any postulated accidents include reactivity events, or other events which could challenge the reactor vessel and reactor system integrity, TCR-23 specifies that "effective cooling" shall be provided, eliminating the need for a separate criterion.	N/A
mHTGR-71	*Reactor building design basis.* The design of the reactor building shall be such that, during postulated accidents, it structurally protects the geometry for passive removal of residual heat from the reactor core to the ultimate heat sink and provides a pathway for the release of reactor helium from the building in the event of depressurization accidents.	TCR-30	*Reactor building design basis.* The design of the reactor building shall be such that, during postulated accidents, it structurally protects the geometry for removal of residual heat from the reactor core to the ultimate heat sink.	See Note 7.

Table A-1. TCR Design Criteria and Comparison to RG 1.232 ARDC/mHTGR-Design Criteria (continued)

RG 1.232		**TCR**		**Notes & Rationale**
DC#	**Title & Content**	**DC#**	**Title & Content, with Highlighted Differences in Red**	
mHTGR-72	*Provisions for periodic reactor building inspection*. The reactor building shall be designed to permit (1) appropriate periodic inspection of all important structural areas and the depressurization pathway, and (2) an appropriate surveillance program.	N/A	Inspection and testing of components is not applicable to the TCR due to its brief deign life.	N/A

Notes:

1. Due to the brief design life (*i.e.*, operation and shutdown periods) of the reactor, most hazards due to natural phenomena can be safely excluded. Therefore, “appropriate consideration” will be significantly less than for a reactor with a 40-60 year design life.
2. Emergency procedures should limit the use of water in the building, around the location of the reactor vessel, especially if there if the status of the reactor integrity or the reactor coolant pressure boundary integrity is compromised, or if it is unknown, to prevent water/steam ingress to the core.
3. Fuel differences between the TCR and mHTGR permit the ARDC version of this criterion as being more applicable than the mHTGR version. However, if TRISO fuel is selected for the TCR, this and other criteria which reference “fuel design limits” will be better served with the mHTGR version over the ARDC version.
4. Like the mHTGR, helium coolant is not expected to affect power and power oscillations. Therefore, coolant terminology has been removed.
5. The ARDC version is chosen over the mHTGR since a passive cooling is not required for the TCR, due to its brief design life. However, the residual heat removal must also be able to provide sufficient cooling under postulated accident conditions.
6. No modifications were made to these criteria due to design uncertainty of the anticipated waste streams, spent fuel storage, and handling aspects.
7. Rapid depressurization of the TCR is not expected to challenge reactor building structures or heat removal safety functions.