Consequence-Based Methodology to Determine Physical Security Requirements for Micro-Reactors

by

Leanne Galanek

Submitted to the Department of Nuclear Science and Engineering
in partial fulfillment of the requirements for the degree of

Bachelor of Science in Nuclear Science and Engineering

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2021

Author .....
Department of Nuclear Science and Engineering
May 20, 2021

Certified by .....
Jacopo Buongiorno
TEPCO Professor of Nuclear Science and Engineering
Thesis Supervisor

Certified by .....
Neil Todreas
KEPCO Professor of Nuclear Science and Engineering
Thesis Supervisor

Accepted by .....
Michael Short
Associate Professor of Nuclear Science and Engineering
Chairman, NSE Committee for Undergraduate Students

Consequence-Based Methodology to Determine Physical Security Requirements for Micro-Reactors

by

Leanne Galanek

Submitted to the Department of Nuclear Science and Engineering
on May 20, 2021, in partial fulfillment of the
requirements for the degree of
Bachelor of Science in Nuclear Science and Engineering

Abstract

Micro-reactors are an emerging advanced fission technology seeking to provide clean energy solutions to aid in the global de-carbonization of energy systems. Without changes to current NRC regulations, micro-reactors may face unduly burdensome on-site physical security costs, leading to reduced economic attractiveness of the technology. A consequence-based methodology is developed and applied to two micro-reactor plants- the Oklo Aurora and the MIT Research Reactor- to better understand if the worst-case consequences of security breaches at micro-reactors warrant the need for onsite physical protection systems. Preliminary results indicate that micro-reactors may be able to prove that, based on inherent plant mitigation features alone, there are no unacceptable radiological consequences associated with any form of security attack on the plant. This would indicate that onsite physical security, including on-site armed guards, may not be necessary for micro-reactors to ensure the protection of the environment and public health and safety.

Thesis Supervisor: Jacopo Buongiorno
Title: TEPCO Professor of Nuclear Science and Engineering

Thesis Supervisor: Neil Todreas
Title: KEPCO Professor of Nuclear Science and Engineering

Acknowledgments

This thesis and the entirety of my undergraduate career at MIT would not have been possible without the love and support of my family. Your encouragement and unwavering belief in me has allowed me to grow to become the person that I am today. Thank you from the bottom of my heart.

I am grateful for all Professor Buongiorno and Professor Todreas have done this past year to lead me through the research process. As an inexperienced researcher, their constant support and advice was invaluable. I would also like to thank Edward Lau and Susan Tucker of the MIT Reactor for their guidance and patience through our many meetings and walk-throughs, as well as in the editing process. Thank you to the members of my research group; Edward James Garcia, Isabel Naranjo De Candido, Lucy Nester, Katherine Zhao and Sara Hauptman; all of whom helped foster a welcoming and supportive research environment. Additionally, I would like to thank Jared Berezin for his encouragement, feedback, and guidance throughout the course of the writing of this thesis.

Finally, I would not have made it through MIT without the support of the friends I have made here. From frisbee and curling, to student radio, late nights psetting, food tours of Boston, and the best roommates and floormates a girl could ask for, the people I've met along my journey have truly been the most rewarding part of my MIT experience. You all deserve as much credit in my graduation as I do and I cannot wait to see all of the amazing things that you do.

Contents

1 Introduction **11**

1.1 Motivation 11

1.2 Objective 12

2 Background **15**

2.1 Micro-Reactors 15

2.1.1 Designs 15

2.1.2 MITR as a Micro-Reactor 16

2.2 Selected Micro-Reactor Designs 17

2.2.1 Oklo Aurora 17

2.2.2 MITR: MIT Research Reactor 22

2.3 Physical Security at Nuclear Power Plants 26

2.4 Current Relevant NRC Regulation 27

2.4.1 Fixed-Site Regulation 28

2.4.2 Transportation Regulation 30

2.5 Alternative Consequence-Based Approach 32

2.5.1 UK Regulation 32

2.5.2 Goals for the Developed Methodology 34

3 Methods **35**

3.1 Overview of Consequence-Based Analysis 35

3.2 Specific Process for Analyzing MITR and Aurora Designs 37

4 Results **41**

4.1 Aurora Analysis 41

4.2 MITR Analysis 44

5 Conclusion **47**

5.1 Results of Consequence Analysis 47

5.1.1 Oklo Aurora Analysis 47

5.1.2 MITR Analysis 48

5.1.3 General Conclusions 48

5.2 Improvements and Future Work 50

A Formal Consequence Analysis **51**

A.1 Analysis Format 51

A.2 Oklo Aurora Consequence Analyses 51

A.3 MITR Consequence Analyses 68

B Dose Calculations **85**

B.1 Oklo Aurora Dose Calculations 85

B.1.1 Dose Based on Modular High Temperature Gas Reactor Study 85

B.1.2 Dose Based on INL Microreactor Study 86

B.2 MITR Dose Calculations 87

List of Figures

2-1 Side view of individual Oklo Aurora Reactor Cell; featuring fuel, reflector, shielding and heat pipe [1] 18
2-2 Top view of individual Oklo Aurora Reactor Cell; featuring fuel, reflector, shielding and heat pipe [1] 19
2-3 Side view of Oklo Aurora reactor cavity; featuring engineered air flow around the cavity to allow for passive decay heat removal [1] 21
2-4 Top cross section of MITR core [2] 23

List of Tables

B.1 Oklo Aurora Dose Calculation 86

Chapter 1

Introduction

1.1 Motivation

A just, or socially equitable, transition from the current global reliance on fossil-fuels requires many different sources of reliable and safe low-carbon energy. To achieve their widespread adoption, these technologies must be economically viable. One such technology, micro-reactors, are very small nuclear reactors that could be used as flexible energy generators for large urban markets, such as district heating; micro-grids for data centers, seaports, airports, and hospitals; as well as mobile and containerized agriculture and manufacturing facilities.

Micro-reactors have thermal power ratings hundreds of times smaller than current, large, light water plants. Their very small size and radionuclide inventory, combined with engineered and passive safety systems, allow micro-reactors the possibility for siting in densely-populated areas. However, this deployment will not be possible without updates to the current US Nuclear Regulatory Commission (NRC) regulations for siting and staffing of nuclear power plants. [3] A major contribution to the onsite staffing requirements for current licensed nuclear power plants is the physical security force.

Following the attack on the World Trade Center on September 11, 2001, enhanced attention was placed on securing and protecting nuclear plants in the United States. Additonally, following the Boston Marathon bombing on April 15, 2013, the threat

of radiological sabotage was realized. [4],[5],[6] The security regulations placed on plants require large forces of onsite physical security, driving up plant operating costs. These current regulations are tailored to larger, older designs and may be unduly burdensome and costly to newer, smaller plants. [7] While a large security force is required for current plants, which occupy large land areas and contain a significant quantity of radionuclides in the core, micro-reactors will be much smaller and often embedded below grade, and thus make less-attractive targets. This insight, combined with innovations in sensing and autonomous control, can lead to cost-effective physical security plans which could reduce reliance on large onsite staffing. Limiting onsite staff will reduce operating costs and allow micro-reactors to compete in the broader energy market.

1.2 Objective

The main purpose of this study is to develop a *consequence-based* security methodology which can be used to develop physical security plans for micro-reactors. This methodology would systematically define the unique consequences of malicious attacks for any reactor it is applied to, allowing the user to understand what must be protected. Once recognized, the reactor developers, owners and operators would be able to design-in layers of physical security to meet the individual plant's needs, allowing flexibility for unique methods as well as broad-reaching regulation. This is in contrast with the traditional prescriptive approach, which mandates a certain number of onsite armed guards and various physical barriers to prevent takeover of the site by an attacking force. The consequence-based methodology is further defined in Section 3.1.

As a case study, the MIT research reactor (MITR) is analyzed to understand its general security methodology. MITR serves as a good case study due to its urban location, comparable thermal power rating to micro-reactors, and its use of local law enforcement (versus dedicated onsite guards) to provide an off-site, readily dispatchable, security force. Through this case study and that of the Oklo Aurora plant, the

minimum requirements for physical security can be assessed, and a consequence-based methodology can be developed.

Other work has been done to assess the security of current plants and even proposed offshore plants. [8],[9],[10],[11] These studies use quantitative methods to evaluate the effectiveness of physical protection systems, address the insider threat, and determine the timeframe of attacks and response systems. However, there are fewer studies which have assessed very small reactors, which serve as low-risk targets and likely pose no excess risk to the public, even in worst-case scenarios. [12],[13]

The insights gained from this study can potentially inform reactor developers, owners, utilities and the NRC on a new, consequence-based physical security methodology for micro-reactors, which allows for right-sized and cost-effective onsite physical security staff, while maintaining adequate protection of public health and safety.

Chapter 2

Background

2.1 Micro-Reactors

Micro-reactors are a class of advanced nuclear reactors. The classification is based on size alone, meaning that there is no specific technology or design required to fit in the micro-reactor class. Additionally, there is no settled definition for the size limits of the micro-reactor class, as the technology is still emerging and there are no currently operating micro-reactors. However, micro-reactors are very small, smaller than small modular reactors, putting their thermal power range at about 100 MW_{th} and below.

2.1.1 Designs

Many companies are currently developing micro-reactor designs. These designs use various advanced fission concepts, including metal-fuels, heat-pipes, and gas-cooling. Some designs are seeking to feature the element of transportability, to allow for the reactor to be transported to various sites and operated for short periods of time, so as to provide aid and relief after natural disasters, or for other end uses. This study will focus on stationary designs, but the developed consequence-based methodology is broad-reaching, and likely could be applied to transportable reactors. Some specific micro-reactor designs include the Westinghouse eVinci, BWX Technologies BANR, X-energy Xe-Mobile, Ultra Safe MMR, and Oklo Aurora.

2.1.2 MITR as a Micro-Reactor

This study will consider the MIT research reactor (MITR) as a case-study of a currently-operating micro-reactor. While micro-reactors are considered to be commercial reactors, the MITR, and research reactors more generally, serve as a good example for micro-reactors to follow for licensing applications. As described in detail in later sections, research reactors follow different and less-prescriptive NRC regulations as compared to commercial reactors. This regulation, specifically for siting and security, is more appropriate for micro-reactors to follow instead of the regulation for commercial reactors, which was developed for larger plants.

MITR, and research reactors more generally, could be classified as micro-reactors based solely on their physical size, low power rating and exceptionally robust safety profile. All currently operating research reactors in the United States are licensed at thermal power ratings of 20 MW_{th} or less. [14] Thus, because they are all below 100 MW_{th}, research reactors fit into the classification of micro-reactors. More specifically, MITR is a very useful case-study for this study due to its location. MITR is sited on MIT's campus, in Cambridge, MA, next to and across from various other Institute buildings, including a graduate student dormitory, and within a half-mile of residential neighborhoods, shopping malls and corporate offices. This urban siting helps to demonstrate that micro-reactors are capable of being deployed in cities and other densely-populated areas, expanding the businesses and locations that could benefit from micro-reactors. This study aims to use insights from current research reactor regulation, which allowed for the siting of MITR in the middle of Cambridge, to understand the requirements for ensuring the safety and security of urban-sited reactors.

The MITR design also offers some interesting similarities and differences with respect to proposed micro-reactor fuels. MITR currently uses highly enriched uranium (HEU) fuel, enriched to $> 90\%$ ^{235}U, for its operations, but is progressing on conversion to low enriched uranium (LEU). Commercial reactors, on the other hand, currently use LEU fuel, enriched to 5% ^{235}U, and micro-reactors will likely use high

assay low enriched uranium (HALEU). HALEU is a popular new fuel concept, which is not as highly enriched as HEU, but has higher enrichment than the fuel used in current plants, thus between 5-20% concentration or "assay" ^{235}U. [15],[16] Fuel is especially important in the security lens, as higher enrichment is generally assumed to need more protection because of its potential to aid in the development of nuclear weapons. [17],[18]

2.2 Selected Micro-Reactor Designs

For the purpose of this study, two micro-reactor designs have been selected to be analyzed more closely, applying the consequence-based methodology. These designs are the Oklo Aurora and the MITR. The Aurora was chosen because of the availability of information for the design due to its recent license application to the NRC. The MITR was selected due to its previously mentioned similarities to micro-reactor concepts, as well as its accessibility.

2.2.1 Oklo Aurora

The Oklo Aurora micro-reactor is a 4 MW_{th} advanced fission reactor. [1] The Aurora design uses Uranium Zirconium (UZr) metal fuel; 19.75% enriched, 90% Uranium and 10% Zirconium by weight. The reactor operates with a fast spectrum and with a low core power density of 3.91 W/cm^3. The core is comprised of 114 hexagonal reactor cells, each cooled by an independent heat pipe. Additionally, within each reactor cell, there are upper and lower zirconium reflectors, an upper gas plenum, and upper axial boron carbide shielding. See Figure 2-1 and Figure 2-2 for more detailed depictions of the Oklo fuel and reactor cells.

The heat pipes, which utilize a potassium coolant, serve as the primary cooling system for the core. Heat generated in the core is transferred via the heat pipes to the secondary system through a heat exchanger. The secondary system is a super-critical carbon dioxide (sCO_2) Rankine cycle, which includes a gas turbine that generates electricity to be used both onsite and offloaded to the grid that the reactor is connected

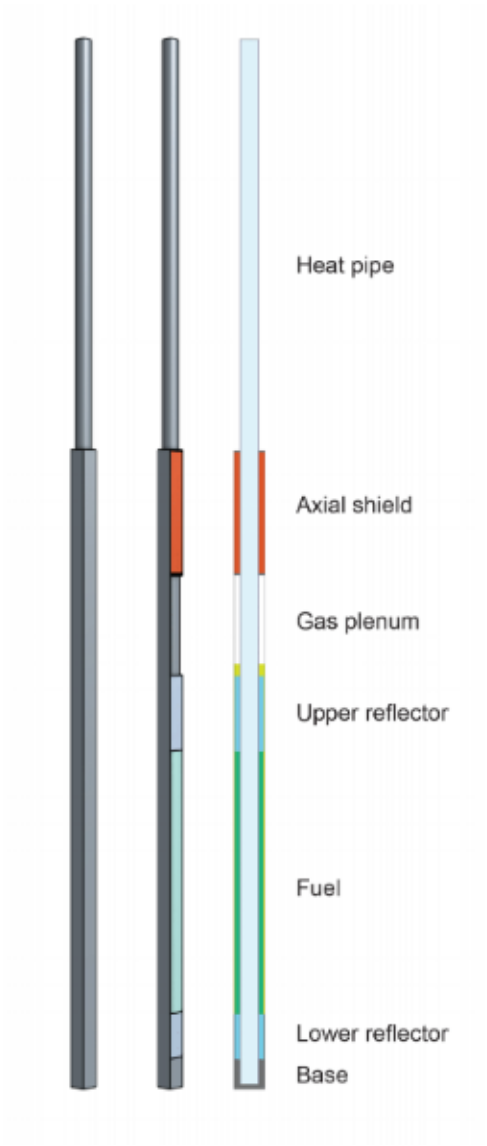

Figure 2-1: Side view of individual Oklo Aurora Reactor Cell; featuring fuel, reflector, shielding and heat pipe [1]

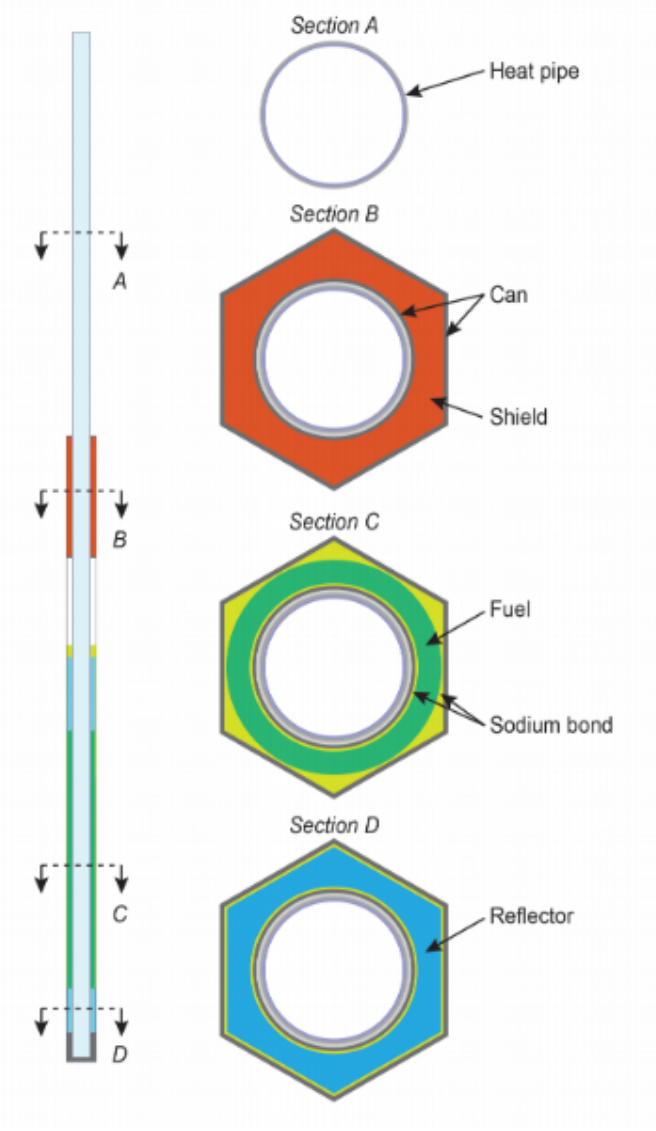

Figure 2-2: Top view of individual Oklo Aurora Reactor Cell; featuring fuel, reflector, shielding and heat pipe [1]

to. Importantly, the Aurora design does not rely on offsite power, and does not offtake any power from the grid. Instead, electricity produced by the plant is used to power the reactor, and a battery, stored onsite, is charged during operation to allow for start-up after any shutdown. In the event that the battery is discharged and the reactor is shutdown, decay heat from the core can be removed passively. The decay heat is transferred through conduction and radiation away from the fuel and to the edge of the reactor cavity. The reactor cavity is cooled by the air in the powerhouse basement, via natural convection, as depicted in Figure 2-3. Thus, the Aurora design does not require power to successfully remove decay heat from the reactor.

Reactivity in the core is controlled through four means: absorbers, reflectors, shutdown rods and control drums. Within the core, there are six absorber cells that form the central ring of the array. These absorber cells have inserts that allow for boron carbide absorbers or steel reflectors to be inserted into the core; depending on if the reactor is being started up or running at normal power. The main reflector for the core encompasses the entire core array and is made of steel. There are three shutdown rods, which during normal operation are suspended above the core via electromagnets. These shutdown rods are each worth at least 1400 pcm, and only one shutdown rod is required to shutdown the reactor. Lastly, there are three control drums, stationed around the edges of the reactor cell array and housed in the outer reflector, which are used to control the reactivity of the core as the fuel depletes. The control drums are comprised of one half Zr reflector and one half boron carbide absorber. The three control drums have a total worth of 700 pcm; about half of one shutdown rod worth. The control drums are rotated via stepper motors, with a rotation limit of $10^{-2} deg/sec$, translating to a 5-hour rotation time to insert the full reflector to face the core. When not rotating, the control drums are fixed in place via an electromagnetic brake. The rotation of these control drums is automatic during normal operation, programmed into the reactor's control logic system.

One of the key innovations of the Aurora design is that it does not require any licensed operators in order to operate. The design proposes to have two onsite monitors, but these monitors do not have actions that are certified in the safety plan;

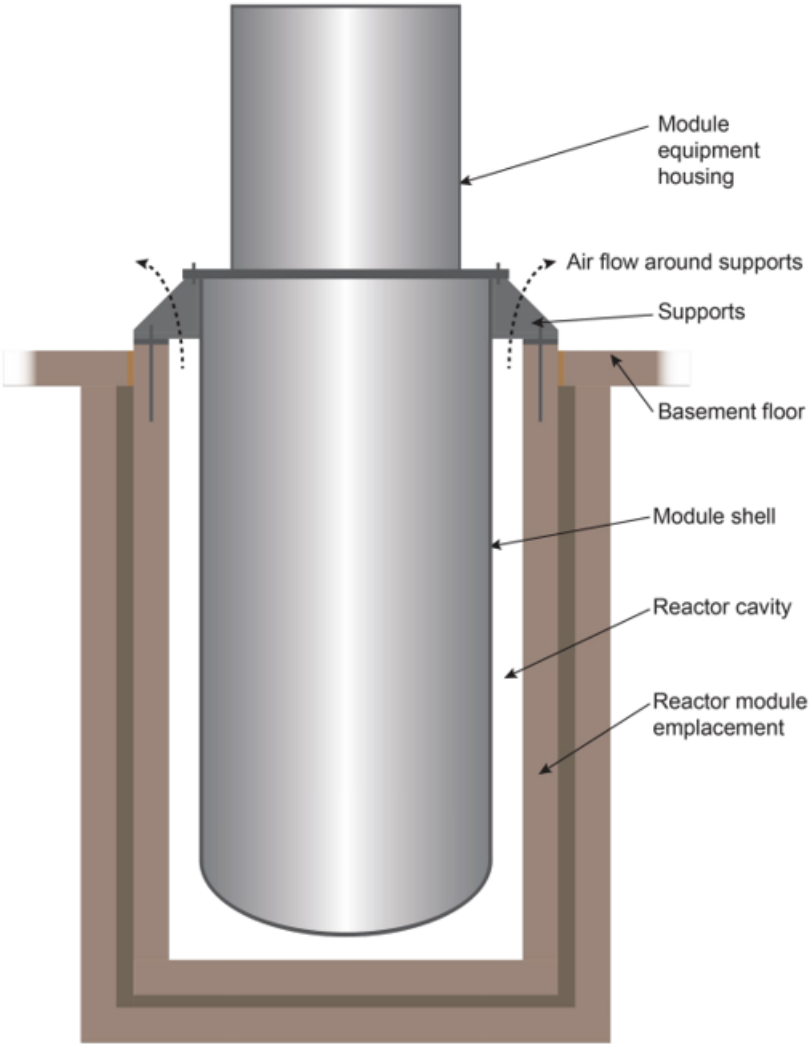

Figure 2-3: Side view of Oklo Aurora reactor cavity; featuring engineered air flow around the cavity to allow for passive decay heat removal [1]

meaning there is no onsite monitor actions that are required for the reactor to operate, or shutdown, safely. Thus, the reactor is largely controlled by logic control systems. These systems use in-core and other plant monitors and sensors to verify that reactor parameters are within their safety limits. If any of these parameters deviate from their imposed limits, then the logic control systems will initiate an automatic reactor trip. A reactor trip signal drops the shutdown rods into the core, shutting down the reactor.

2.2.2 MITR: MIT Research Reactor

The MIT research reactor (MITR) is a 6 MW_{th} light-water cooled and light-water moderated fission reactor. [2] MITR utilizes highly enriched, cermet Uranium Aluminide (UAlx) plate-type fuel. These fuel plates are housed in fuel elements of rhomboidal cross section. Each fuel element contains 15 fuel plates and there are 27 slots for fuel elements in the hexagonal core. During normal operation, there are 24 fuel elements in use, while the other 3 slots are used for experiments. These fuel elements are arranged in 3 distinct rings, as shown in Figure 2-4. The hexagonal core sits inside a light-water core tank, which itself is surrounded by a heavy water (D_2O) reflector tank. The D_2O tank is surrounded by a graphite reflector, which is in turn surrounded by a lead-steel thermal shield. Lastly, a biological shield of heavy-dense concrete surrounds the thermal shield. The overall core diameter is 20 feet (6.1 meters). A light water secondary system removes heat from the core via nine heat exchangers, and rejects this heat to the environment via cooling towers.

The MITR is a university-based research reactor, and as such, is regularly used for experiments. Some of these experiments include in-core experiments that take the shape of fuel elements, such as the In-Core Sample Assemblies (ICSA). These ICSAs are contained in structures that are the exact same shape as fuel elements, allowing them to be integrated into the hexagonal fuel assembly. When in use, these ICSAs replace some of the fuel elements in the core. Another key experimental feature is the automatic transfer system. This system consists of pneumatic tube systems that can be used to send samples to be irradiated very close to the core. The MITR features

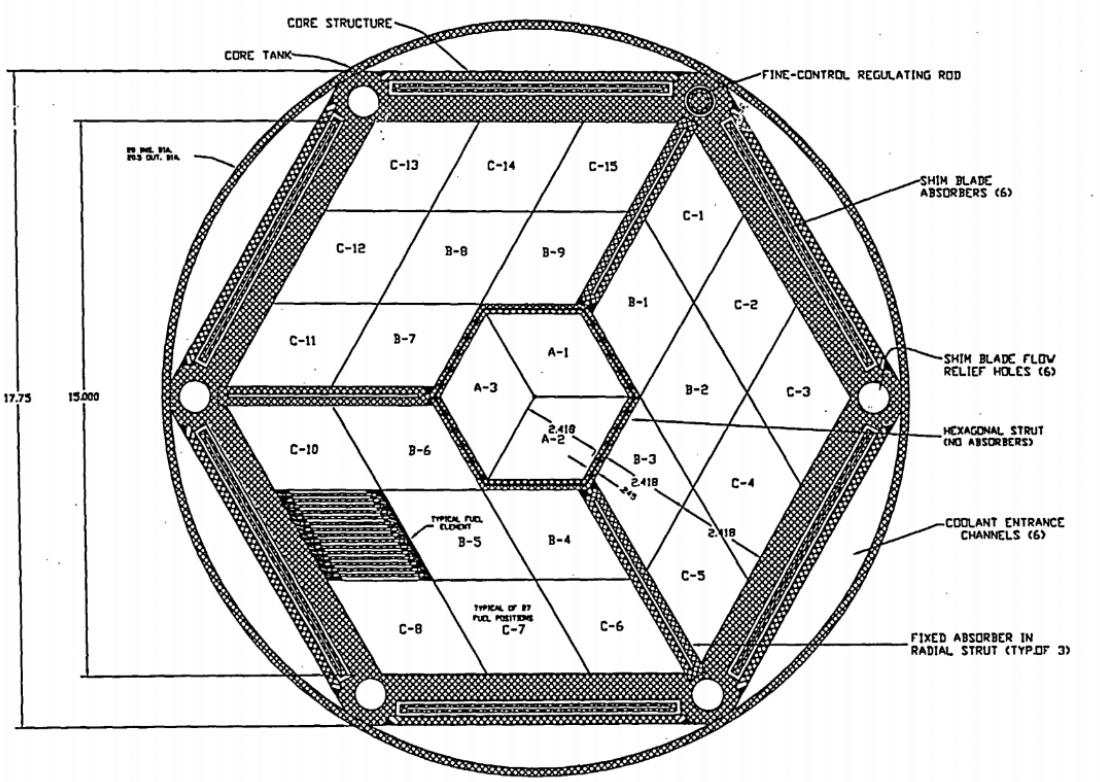

Figure 2-4: Top cross section of MITR core [2]

many other experimental features, including beam ports, a hot cell facility, a fission converter and a basement medical irradiation room.

Reactivity of the MITR core is controlled via four major systems. First, six boron impregnated stainless steel shim blades are positioned at the edges of the hexagonal fuel array. These shim blades are responsible for shutting down the reactor during a scram, whereby they are dropped from their drive mechanisms into the core. Each shim blade has its own drive mechanism and electromagnet; the electromagnet is de-energized in a scram, allowing the blade to drop freely into the core. During normal operation, these shim blades are controlled manually via levers in the control room. Second, a cadmium regulating rod, also located on the periphery of the fuel array, is used to fine tune the power level of the reactor. This control is accomplished either manually via a switch in the control room, or via automatic control by the reactor's digital automatic control system. Third, there are two reflector systems; a heavy water reflector tank and graphite reflector. The D_2O reflector tank uses forced flow to circulate the heavy water through a heat exchanger, to help remove heat from the core. Beyond providing some core cooling, the D_2O reflector also has substantial reactivity worth, and has the ability to render the reactor subcritical. This occurs when the D_2O reflector is dumped; the tank is rapidly drained to a storage tank below the core and thus substantially reduces the neutron economy in the core and shuts down the reactor without any dropping of shim blades. Lastly, the MITR core also features fixed absorbers. These boron stainless steel fixed absorbers, located in the upper half of each fuel element, ensure an appropriate shape of the neutron flux for experiments under the core, such as the basement medical irradiation room.

There are a few key engineered safety features at MITR. One of these is a full containment, chosen because of the urban siting of MITR. The containment is a domed cylindrical air-tight and water-tight structure. The domed part of the structure is built of 5/8-inch steel plate, while the cylindrical part is built of a 2-foot thick concrete wall surrounded by 3/8-inch steel plate. This containment has two of its own important engineered features. The first is the containment isolation system, which prevents the release of fission products. Exhaust ventilation from the containment

building flows through a holdup plenum before being expelled to the environment. Radiation monitors are positioned at the entrance to the plenum, and when high levels of radiation are detected, dampers at the exit to the plenum are triggered to close. In this case, dampers at the entrance of plenum also close, sealing the plenum to prevent release of radioactive effluents to the environment or back into the containment. There are 2 redundant damper systems: a main system controlled hydraulically, and an auxiliary system controlled by gravity. The auxiliary dampers close if the main dampers take too long to close, and both sets of dampers close automatically with a loss of power. The second containment feature is the containment pressure relief system. This system is used to maintain sub-atmospheric pressure in the containment building once the containment is isolated. Maintaining sub-atmospheric pressure inside the containment is important when trying to prevent any leak-out of unfiltered radiological effluents trapped inside the containment building. This pressure relief system is manually activated and can be initiated from outside of the containment. The system processes and removes radioactive particulates from the containment air before its vented release to the environment. This processing focuses on the removal of radioactive Iodine and releases 100% of noble gases and Br, less than 1% of I, and 50% of all other fission products. The final important engineered safety feature of MITR is the Emergency Core Cooling System (ECCS). The ECCS sprays water onto the core at a rate sufficient to remove decay heat. ECCS has two redundant nozzle systems and must be initiated manually, either from the control room or outside of the containment building.

Additionally, because the MITR is currently operating, the reactor already has a set, NRC-approved, security program. Similar to other research reactors in the United States, the MITR is not required to have any onsite security guards, and instead relies on the campus police department to provide an armed response force in the event of an emergency. The MITR security plan specifies a specific time window in which the police force must be able to respond to the scene, and thus the systems in place onsite are meant to delay an attacking force enough to allow the MIT Police to arrive before any serious damage is done. This onsite physical protection system

includes surveillance cameras; intrusion detection alarms; and physical barriers such as fences, airlocks and doors that stay locked at all times except for authorized access.

The MITR is operated by licensed reactor operators, and at any time while the reactor is operating there must be at least one reactor operator and one senior reactor operator onsite. However, these are the only two persons required onsite during operation. The reactor operators can perform power level adjustments, as well as shutdown and restart the reactor. Importantly, the reactor protection system will automatically scram the reactor during certain unsafe conditions. The reactor protection system monitors reactor power, period, coolant outlet temperature, coolant flow and core tank level. This system uses coincidence logic, meaning the system will generate a scram signal if multiple instruments monitoring these reactor parameters detect an unsafe level. An unsafe level means that the reactor parameter has fallen outside of specified setpoints. The MITR has 3 types of shutdown: a minor scram, which drops all shim blades; a major scram, which drops all shim blades, dumps the D_2O reflector and isolates the containment building; and a dump of the D_2O reflector alone, which can shutdown the reactor without shim blade drop.

Similar to the Aurora, the MITR can also remove decay heat from the core passively. On the loss of forced flow through the core, natural convection valves and anti-siphon valves in the core tank open, allowing for a pathway of natural circulation of coolant through the core. This natural circulation provides enough cooling that decay heat is removed passively, without onsite power or working coolant pumps.

2.3 Physical Security at Nuclear Power Plants

The security of nuclear power plants has always been a major concern throughout the history of their licensing and operation, even before the 9/11 attacks. The overall goal for the security of plants is to protect the health and safety of the public and the environment by preventing the malicious use of radioactive materials. To this end, the two main events that must be protected against are theft and sabotage. Theft refers to the unauthorized removal of radioactive materials from a site, including

removing fuel, spent fuel, and/or irradiated materials. Radiological sabotage refers to any malicious action which causes a disturbance to the normal operation of a plant, including causing reactivity excursions, core damage, or the release of radionuclides to the environment. The US Nuclear Regulatory Commission (NRC) has developed regulations that all licenses must abide by, in order to ensure that the US fleet of reactors is safe and secure. This regulation is quite prescriptive, meaning that there is little flexibility for plants to design their own security programs; instead they achieve security by meeting regulations.

It is important to make the distinction that this study is focused on the physical security, versus general security, of micro-reactors. Security at nuclear power plants, in general, encompasses many different programs. These include cybersecurity, quality assurance, security culture, employee readiness/fitness for duty, and access control. [19] While these programs are all essential to ensure the overall security of the plant, this study focuses on physical security, or the physical equipment on site that must be protected and maintained in the event of a security breach.

2.4 Current Relevant NRC Regulation

The current NRC regulation uses a graded-approach to physical security, meaning that the amount of security required at a site is based on the type of facility, and further the perceived risk of the facility. Importantly, this means that the NRC has different physical security regulations for commercial power plants and research reactors. As previously mentioned, this study recognizes the closeness between research reactors and micro-reactors. Due to their comparable size and power rating, which generally have been thought of to relate to the risk of the facility, the regulation for research reactors displays how the NRC imposes and verifies physical security regulations at facilities similar to micro-reactors. Lessons about the types and strength of physical security systems needed at research reactors serve to inform developers of micro-reactor security systems.

The outcome of this study, the consequence-based approach to physical security,

can be applied to both fixed site operations and in the transportation of micro-reactors. Thus, current regulations on both topics are gathered and synthesized.

2.4.1 Fixed-Site Regulation

Fixed site regulation uses four main principles to ensure protection against theft and radiological sabotage. These are: detect, delay, assess and respond. Thus, a site's security system should be able to detect any intruder/threat, delay the threat as much as possible, assess the threat and determine the best plan of response, then finally respond to the threat with the force required.

10 CFR Part 73

Most of the NRC regulations specific to physical security are housed in 10 Code of Federal Regulations (10 CFR) Part 73. [3] More specifically, sections 73.45, 73.46, and 73.55 provide the requirements for physical security at fixed sites. These sections set specific and prescriptive requirements for sites that house nuclear power plants. Section 73.45 details the necessary performance capabilities of physical security systems onsite to prevent unauthorized access to the site and the nuclear material onsite. The systems responsible for preventing this access include physical barriers, monitoring and communication systems, and an armed response force. Section 73.46 goes a step further and identifies those site systems and sub-systems, then lays out specific requirements for them. This section also details strict requirements for procedures and personnel that must be onsite at all times during operation.

One of these strict requirements is the necessity for onsite alarm stations. These alarm stations serve as a hub where the alarms for all intrusion detection systems, as well as live camera feed, are displayed. The stations are continuously manned, so as to constantly allow understanding of the state of security at the plant. The alarm stations also serve as communication centers, allowing for a site to contact offsite local law enforcement for help in the event of a security breach, via telephone or two-way radio. NRC regulation requires two onsite alarm stations per site, to ensure

that no single adversary action can destroy the capability to notify offsite response. Additionally, alarm stations must remain operable with the loss of offsite power, and must be tested regularly to ensure operability.

10 CFR Part 73.46 also imposes the requirements on physical barriers onsite. The regulation requires at least three barriers between the site boundary and the core. These barriers serve to deter and delay attackers, while also creating a system for identifying areas bounded by these barriers. Using the barriers to distinguish certain zones onsite, the regulations impose further requirements for each zone in terms of allowed personnel and procedures within each.

10 CFR 73.55 is focused on radiological sabotage. This regulation uses the design basis threat (DBT) methodology and requires licensees to identify site-specific target sets, classify vital areas, and build in security to protect them. The DBT method requires that a site consider specific attacking threats defined by the NRC, as well as through specific routes (i.e., vehicle, sea). These threats specify the size, training and weaponry of the attacking force, and thus physical security is designed with the force in mind. Because of this, Part 73.55 requires at least ten armed responders onsite at all times for a commercial plant, in order to provide a defending force during an attack. Importantly, this onsite armed guard requirement is not imposed on research reactors, and thus they do not utilize armed guards onsite. This is a key distinction because micro-reactors licensed under the current commercial reactor plant regulations would be forced to have 10 armed guards onsite, and to pay for those workers, when this force may be shown to be unnecessary.

There have been proposed updates to the NRC regulations for physical security at micro-reactors in the past few years. [20] These proposed rulemakings would eliminate the requirement for any onsite physical security, and would allow micro-reactors to rely on offsite, contracted security or local law enforcement, to provide an onsite response in the event of a security breach. This form of offsite response is exactly the model that research and test reactors use. MITR, for example, relies on the campus police force, MIT Police, to act as their offsite response in case of emergency. Even more recently, the NRC has released documents suggesting that

grouping micro-reactors with research and test reactors is sensible, especially for physical security regulation. [21] The NRC staff has also expressed that prescriptive staffing and operational requirements may be too extensive for micro-reactors. [22]

10 CFR Part 37

New NRC physical security regulations were published in 2013 and are found in 10 CFR Part 37. [23] Licensees that utilize the most "risk-significant" quantities of radioactive material must follow Part 37, which includes both commercial and research reactors. [24] Facilities that follow Part 73 and develop a security plan are exempt from Part 37 requirements. While micro-reactors would likely follow Part 73 (not Part 37) regulations based on the precedent that currently operating plants follow Part 73, Part 37 regulations offer a less prescriptive example for licensees to follow to understand the purpose of security systems and at this stage, there is the potential that new plants could choose to follow Part 37. Part 37 uses a graded security approach in which facilities that have more nuclear material or utilize material more attractive to adversaries require more security. More importantly, Part 37 regulation places more of the burden of proof that physical security systems are adequate for the threat and risk of the specific facility, in the hands of the licensees themselves. This is different than Part 73 regulation, which imposes strict security programs to implement and maintain, ensuring security through meeting specific regulation, rather than making licensees determine what security programs their site needs.

2.4.2 Transportation Regulation

One of the distinctions for micro-reactors, being as small as they are, is that they can potentially be shipped as a whole unit. Traditionally, nuclear power plants have been intensive construction projects, building the plant from the ground up at the site, and later shipping the fuel to the site separately. Micro-reactors could potentially be built and fueled off-site, at a commercial facility, then transported to the site. Upon refueling, the whole expended core of a micro-reactor could be replaced by a fresh

new core. This would allow micro-reactors to be fully re-fueled offsite, eliminating the need for long refueling outages.

10 CFR Part 73

10 CFR Part 73 also features physical security regulations specific to the transportation of radioactive materials. Sections 73.25, 73.26 and 73.37 provide the requirements for shipping both fresh and spent nuclear fuel. Part 73.25 requires licensees to pre-plan the shipment itinerary, and prevent unauthorized access to the shipped materials before and during shipment, through the detection, delay and response to threats. Part 73.26 adds further detail: licensees should strategically schedule the shipment to avoid traffic, natural disasters, and civil disorders; and the response force during shipment of radioactive materials must include at least seven armed guards and a convoy of vehicles, including the cargo vehicle plus two separate escort vehicles, all of which are in constant communication with a designated movement control center. Part 73.37 adds additional requirements for the shipping of spent fuel, including the need for armed responders to carry two weapons each.

Other Transportation Regulations

Several other sources provide regulations for the transportation of nuclear materials. These include 10 CFR Part 71, 49 CFR Part 171, and the International Air Transport Association (IATA) Dangerous Goods Regulations. [25],[26],[27] Together, these regulations describe the methods for determining what types of packaging must be used to ship various types and quantities of nuclear materials. The packaging has strict testing and labeling requirements, but the regulations would allow for a micro-reactor to be shipped as a singular package, by rail, sea and air. The shipping company would need to have security training and a security plan would need to be developed for each shipment, but conceptually it could be done.

2.5 Alternative Consequence-Based Approach

As described, the current NRC regulation is very prescriptive, and if micro-reactors are forced to be licensed under this regulation, the requirements imposed may be unduly burdensome, and further the cost of the security program could prevent the reactors from being economically attractive. Thus, this study seeks to develop an alternative approach which is focused on looking at the specific consequences of a security breach at a reactor, and determining from that analysis what types of physical security must be built in to prevent unacceptable consequences. This approach is to be referred to as a consequence-based approach and is fully defined in Section 3.1.

2.5.1 UK Regulation

The United Kingdom recently adopted a consequence-based approach to security, in 2017. [28] The United Kingdom's regulator, the Office for Nuclear Regulation (ONR), has developed one security approach that is applied to all of the country's nuclear facilities, from nuclear power plants to medical isotope facilities. In this outcome-focused regulation, the ONR has developed 10 Security Assessment Principles (SyAPs) to define the general security programs that every plant should include. [29] Within each of these SyAPs, the ONR has further defined the desired outcomes of each of the programs through the security delivery principles (SyDPs). [30] [31],[32],[33] Thus, the UK regulation has no prescriptive requirements. Licensees craft security programs with the guidance of the SyAPs and the understanding that whatever they choose to create must meet the SyDPs.

One of the ten SyAPs is Physical Protection Systems. This principle explains that a security program should incorporate a "proportional" physical protection system that integrates technical and procedural controls to build layers of security. These controls build defense-in-depth and are graded according to the potential consequences of a successful attack. Within this Physical Protection Systems SyAP, there are seven SyDPs, two of which are important to this study: categorization for theft and categorization for sabotage. [34],[35]

The focal point of the consequence-based analysis is the categorization of facilities for theft and for sabotage. In the case of theft, licensees need to identify the quantities and forms of nuclear material that will be on site over the course of the plant's lifetime. Once this information is identified, the site is categorized for theft based on the attractiveness of the material onsite, and the potential consequences of the material being stolen. This measure of attractiveness is determined by the potential malicious uses of the material; the most attractive material could be used to build a nuclear weapon, a dirty-bomb or a radiological exposure device. A dirty-bomb is a device that uses traditional explosives, such as TNT, to explode and disperse radioactive materials in a targeted area. A radiological exposure device is a device that can be placed in a highly-trafficked public area, which uses the inherent activity of a source to expose members of the public to radiation. The licensee should consider inherent characteristics of a material that could detract from its attractiveness, such as the dilution, dispersion, type and form of the material, translating to how easily the consequences can be accomplished. Thus the threat of theft is categorized by the severity of the consequences of the theft and subsequent malicious use of the material. The ONR has developed a classification chart for the threat of theft, mapping the consequences to specific security outcomes that must be accomplished if certain consequences are possible. Thus, the required security is based on the risk associated with the facility. Unfortunately these tables are not publicly available, but the general methodology of such a consequence table is important.

Similarly, the categorization for sabotage is also based on the risk associated with the facility. In this case, licensees need to identify the number and size of vital areas onsite. A vital area is defined as "an area containing nuclear material or SSCs [structures, systems, and components] that if sabotaged result in unacceptable radiological consequences." [35] These unacceptable radiological consequences (URCs) are defined by the ONR, and translate to dose limits onsite and at site boundaries. Once the vital areas are identified, the facility is classified based on the number and size of vital areas onsite; the larger the vital areas and/or the more of them, the more protection a facility will require, because these vital areas can be thought of

as targets of an attacking force. This classification again defines security outcomes that must be accomplished by facilities with certain levels of risk, determined by the number and size of targets onsite. As was true for the classification for theft, the exact classification of unacceptable radiological consequences and vital areas is not publicly available, but the general methodology is important.

2.5.2 Goals for the Developed Methodology

The main goal for the developed consequence-based methodology is to provide a method for evaluating the need for security at a site based on the inherent characteristics of the reactor and plant design. The analysis of each site will ignore any designed security systems; in fact, this methodology should be applied to developing reactor and plant designs to attempt to engineer out potential consequences. [19] This so-called "security by design" is an important concept for micro-reactors, which are currently under development, and can use the developed methodology to efficiently develop and implement security programs.

Chapter 3

Methods

3.1 Overview of Consequence-Based Analysis

The general methodology of the consequence analysis is to assume that an attacker is in control of the facility, and then determine the worst-case scenario consequences that their attack can cause. This approach is different from other current methods for evaluating security at nuclear facilities, as it assumes an attacker is always able to gain control of the plant and can disable any security element or system they have the technical ability to interdict. In this way, consequence analysis obviates any use of a design basis threat (DBT) or other method of determining the probability of an attacking force gaining access to and control of a facility. [36] Importantly, this approach also does not take credit for interdiction by any security systems at the facility or intervening actions by onsite staff. Instead, the analysis focuses on only the inherent features of the plant: what are likely to be the targets of an attack and what about the plant inherently prevents, diminishes, or delays these attacks. Once the unique consequences of the facility attack are enumerated, these consequences are examined to determine whether or not they are acceptable. If the consequences are significant and have an adverse effect on public health and safety, then security systems must be designed and implemented to prevent such consequences from occurring. In the case of the current fleet of larger reactors in the United States, these security systems always include an onsite response force, because the consequences to

the site are considered unacceptable and thus must be prevented with a high degree of confidence.

To frame the consequence analysis of micro-reactors, lessons learned from the new UK consequence-based regulation were considered. [29] The understanding of these lessons, that the two main concerns of every nuclear facility are theft and sabotage, led to this study's development of a list of security concerns that are applicable to all micro-reactors. [34],[35] There are five basic concerns that must be evaluated for every micro-reactor, two pertaining to theft and three pertaining to sabotage. The concerns are as follows, asking, if an adversary is in control of the facility can they:

1. Steal radioactive material (fuel or full reactor) from the site? What can be done with that material? How easily?

2. Steal sensitive nuclear information? (i.e., site layout, patrol schedules, security plans, etc.)

3. Cause a reactivity excursion? What systems, equipment or controls would cause this?

4. Interrupt removal of residual heat and cause fuel degradation? What systems, equipment or controls would cause this?

5. Breach the containment shell and subsequent barriers with explosives? How close must explosives be to cause dispersal of radionuclides from the core?

To conduct the consequence analysis, adequate knowledge of the design of the facility, including the reactor and secondary system design and layout, must be known. Then, systematically, each potential concern must be considered, and analysis must be done to determine if the concern is credible. If the concern is credible, meaning it is feasible that an attacker could produce the concern, then further analysis must be done to detail the pathways through which the attacker can cause this outcome. Next, the consequences of the outcome must be hypothesized, in terms of plant damage, radiological release or loss of fissionable material. Finally, these consequences must

be compared against pre-determined standards of acceptable versus unacceptable consequences. If consequences are acceptable, then no further action must be taken. However, if the consequences are unacceptable, physical security systems must be added to protect against the concern and subsequent consequences.

It must be noted that this consequence analysis, while different because of its lack of use of a DBT, draws heavily from current security approaches. Specifically, when evaluating threats of sabotage, the analysis follows the vital area identification methodology, used by both the NRC and the International Atomic Energy Agency (IAEA). [3],[37] In the case of this study's consequence analysis, vital area identification helps to determine the pathways through which sabotage concerns can occur. Normally vital area identification uses more technical and detailed analysis than this study does, but the general concepts for identifying target sets is a large part of the consequence analysis.

3.2 Specific Process for Analyzing MITR and Aurora Designs

In order to analyze the two chosen designs, the MITR and Oklo Aurora, the Final Safety Analysis Reports (FSAR) for each reactor were read and analyzed. An FSAR is a document used by the NRC for licensing reviews. It is developed and submitted by the owner of the plant, and includes detailed descriptions of the reactor design, including all of its safety systems, cooling systems and secondary systems. It also presents the reactor's most challenging safety cases, as determined by the applicants. This bounding analysis is very useful to understand, as it includes the specific pathways by which the reactor ends up in its most challenging state. From this bounding analysis, the consequence analysis can begin. Pathways to achieving the most challenging state can be determined, and due to the bounding analysis, the consequences of such pathways are already known. After determining these initial pathways, the consequence analysis must then go further to identify all possible pathways for the

given concern. These pathways may not be included in the FSAR, since the FSAR is focused on safety and not security. Safety analysis assumes systems work with a given probability and failures of these systems can be quantified. Thus, if failure rates are low, certain pathways may not be considered in the safety analysis, as they are highly improbable. This is not true for security events, since through sabotage, systems can be disabled regardless of how reliable they are in normal operation. With this in mind, it should be determined if attackers can reasonably attack plant systems and disable them. This will generate some possible pathways that lead to security events that are not possible safety events. Consequence analysis must push to consider these security-only pathways, to generate an exhaustive list of all possible attack sequences leading to theft or sabotage.

After the pathways to the selected concerns are determined, mitigation features preventing each of the outcomes should be identified. These mitigation features include inherent plant features, such as fuel or moderator thermal properties, as well as engineered features of the reactor design, such as physical barriers between the core and public or decay heat removal mechanisms. From there, considering both the identified pathways and inherent mitigation features, consequences for each concern should be hypothesized. These consequences should be identified via known fuel quantities and composition, to get an accurate picture of the worst-case radiological releases or possible nuclear weapons designed from theft. The last aspect of the consequence analysis is to identify the timeframe of each concern. This timeframe includes both the time required for the attack as well as the timing of the plant response. By developing this timeframe security systems can be designed to add delay and deterrence, to allow the plant response to prevent any consequences occurring before offsite response forces can arrive.

Once the consequences for each concern are determined, they must be compared against a set standard to determine if they are acceptable or unacceptable. In the case of this study, a 25 rem dose limit at the site boundary has been chosen as the standard to compare the determined consequences to. This limit comes from the previously mentioned, recently proposed, NRC Part 73 rulemaking, which would allow small

reactors to rely on offsite security (instead of onsite armed guards) provided they meet these dose limits. [20] This proposed rulemaking was released in 2020 and is expected to be finalized in 2022. [38] One other potential dose limit that could be used, but was not chosen for this study, is a 1 rem dose limit at the site boundary. This limit comes from a recently approved revision to NUREG 1537 under the Non-Power Utilization Facility (NPUF) Rule. [39] Under this NPUF Rule, the 1 rem dose limit serves as a marker to classify non-power reactors, which are subject to less consuming and less restrictive regulation as compared to commercial reactors. By using this 1 rem dose limit in a consequence analysis, micro-reactors may be able to argue to be treated like NPUFs in the eyes of regulation. This study chose to use the 25 rem dose limit instead of the 1 rem dose limit because the 25 rem dose limit is directly linked to recent NRC security regulation, and if approved would immediately apply to micro-reactors, whereas the NPUF rule does not yet apply to a commercial micro-reactor.

Chapter 4

Results

4.1 Aurora Analysis

For the consequence analysis of the Aurora design, the FSAR and all attachments (technical specifications, emergency plan and requested exemptions) were analyzed. [1],[40],[41],[42] The Aurora's most challenging safety cases are a reactivity insertion event and a loss of heat sink event. The reactivity insertion event is caused by the rotation of control drums until the reflector is fully facing the core, inserting excess positive reactivity. The loss of heat sink event can be caused by numerous things: failure of heat pipes, turbine trip, sCO_2 pump trip, ultimate heat sink malfunction, sCO_2 safety valve actuation, and sCO_2 pipe break. Out of all of these events, the bounding case is the loss of heat sink cause by a sCO_2 pipe break. However, even in this bounding event, the Aurora FSAR assumes that the reactor can safely shutdown, and all decay heat can be removed passively through conduction to the reactor vessel and convection to the air surrounding the reactor vessel. As such, the FSAR states that no credible accident within the safety analysis, including the flood, fire, explosion, and earthquake analyses, leads to radiological release.

As a part of the bounding analysis, it is assumed that one of the shutdown rods fails. But, because there are three redundant shutdown rods and only one is needed to successfully shutdown the reactor, this singular failure would not prevent the reactor shutdown. Because shutdown is assumed to occur in any safety event, based on the

extremely low failure rate of the shutdown rods, the consequence analysis needed to consider events where the reactor was prevented from achieving safe shutdown. Additionally, a new concern was identified for the Aurora design: can an attacker restart the reactor? If the reactor is successfully shutdown at first, due to the attack, it is important to understand if the adversary can restart the reactor and proceed with their sabotage.

This consequence analysis assumed that the worst-case scenario of a sabotage event, if there are credible pathways for the concern, is a radiological release from the core. To estimate the magnitude of this release, two different studies were surveyed. [43],[44] One of these studies was of modular high temperature gas reactors (MHTGR), and the other was of a molten salt micro-reactor. The results of these studies were scaled by thermal power rating to compare to the 4 MW_{th} size of the Aurora. The final scaled dose results are considered to be the worst-case scenario outcome for sabotage events, where all fission products generated in the core are released to the environment outside of the powerhouse building. The derivation of these doses can be found in Appendix B, Section B1, and are summarized as follows:

- Dose based on MHTGR study:
  - Worker: 1,664 rem
  - Public: 3.03 rem
- Dose based on INL molten salt micro-reactor study:
  - Worker: 3,100 rem
  - Public: 50.8 rem

There are a few important details that must be noted concerning these developed doses. Firstly, for the MHTGR doses, the original study from which the doses were developed provided data in the form of source terms. Thus, dose conversion factors were used to convert these source terms into doses. [45] This use of dose conversion factors generated a separate dose for members of the public versus individual onsite

plant workers, which is assumed to be based on distance to the source of radionuclides (the core). Importantly, the numbers that the dose calculations start from, the source terms, don't account for the system release fraction, dispersion and attenuation, or dose pathways, all of which would change the effective exposure, if considered.

For the molten salt micro-reactor doses, the original INL study assumed a co-located worker at 100 meters and an off-site member of the public at 4,700 meters. These distances are very different than the Aurora site boundary distance of 8.5 feet (2.6 meters). Scaling the doses back from 100 meters to the distances of the Aurora would result in significantly higher doses and would have questionable reliability due to the effects of wake effects around buildings at very close distances. Thus, these dose calculations are again only meant to be guiding values.

At the end of each consequence analysis, these final scaled dose results were compared to the chosen metric for unacceptable radiological consequences. This metric is 25 rem total effective dose equivalent at the site boundary, which for the Aurora is only 8.5 feet (2.6 meters) at the shortest point. It was determined from the Oklo consequence analysis that the outcomes of all of the sabotage concerns (i.e., reactivity excursion, interruption of heat removal systems, breaching the containment with explosives) would likely lead to unacceptable radiological consequences based on one study's doses but not the other. Thus, some forms of physical security systems may need to be incorporated at the site in order to prevent these consequences. This prediction of unacceptable radiological consequences is extremely conservative because it is determined using outside studies rather than known Aurora plant data or calculations, and the two studies do not reach the same conclusion. Thus, this analysis should be considered only as a guide, with future work to be done to refine the analysis. The formal, detailed consequence analysis for each of the given concerns for the Aurora design is summarized in Appendix A, Section A2.

4.2 MITR Analysis

For the consequence analysis of the MITR design, the FSAR was analyzed. [2] The MITR's most challenging safety case, identified by its FSAR as the maximum hypothetical accident (MHA), is a coolant flow blockage in the fuel element with the hottest fuel plate. The blockage is assumed to be caused by a foreign object that falls into the core tank, through the lower grid plate, during refueling when the element position is open. The object would need to pass through the fuel element nozzle opening, so it is limited in size. During the MHA, it is assumed that the entire active portion of 4 fuel plates, in one fuel element, melt. The MHA analysis predicts that this fuel melt would result in a whole-body dose at the site boundary of 247 mrem in a 2-hour period.

The MITR analysis, like that of the Aurora, also includes the concern regarding the attacker restarting the reactor. This is because the MITR's reactor protection system can automatically scram the reactor for various safety concerns, so the restart must again be considered. Additionally, the sensitive nuclear information concern is not considered for MITR, largely because the FSAR does not mention anything about information control. From interviews and walk-throughs at the MITR, it is clear that there is certainly information control at MITR. However, the intention of this study is to perform a consequence analysis based on only the inherent design of the reactor, as described in the FSAR.

This consequence analysis assumed that the worst-case scenario of a sabotage event, given there are credible pathways, is a radiological release from the core. To estimate the magnitude of this release, the given release for the MHA is scaled for a full-core melt. Further details for this calculation can be found in Appendix B, Section B2. The predicted dose for a full-core melt is 22.23 rem, which is within the limits for acceptable consequences. Thus, based on this study, MITR would not need to utilize physical protection systems onsite. As previously mentioned, the MITR does have a formal security plan, including an offsite response force. But this consequence analysis helps to justify the use of this offsite, rather than onsite, force, given that

the potential consequences are not severe enough to be unacceptable. Again, this consequence analysis is extremely conservative, and thus should be considered only as a guide. The formal, detailed consequence analysis for each of the given concerns for the MITR is summarized in Appendix A, Section A3.

Chapter 5

Conclusion

5.1 Results of Consequence Analysis

The consequence analysis reveals preliminary results that can be expanded and refined in future studies.

5.1.1 Oklo Aurora Analysis

For the Oklo Aurora analysis, the consequence-based methodology revealed that a worst-case scenario release from an act of radiological sabotage may exceed the chosen unacceptable radiological consequences. This result should not be taken as final; the quantitative dose calculations used for this analysis were extremely high level and developed from multiple outside sources, but not Oklo itself. Further, the results from the separate sources did not agree, with only one of the two predicting unacceptable radiological consequences. A more detailed calculation would need to be done to determine the potential release in the event that the reactor cannot scram, using known fission product quantities and taking into account the barriers between the fuel and the environment.

5.1.2 MITR Analysis

For the MITR analysis, the consequence-based methodology revealed that a worst-case scenario release from an act of radiological sabotage likely would not exceed the proposed limits for dose to the public. Again, as with the Oklo analysis, these derived dose calculations should not be taken as final, since they are extremely conservative and overly estimated. That said, the MITR dose calculation was based on the MITR FSAR's MHA calculation, and as such is likely a more accurate portrayal of dose as compared to the Oklo calculation. This MHA calculation includes the specific details needed to get a good dose calculation, including site and operation-specific dose calculations, release fractions for barriers between the fuel and the environment, among other details.

An important concept that the MITR analysis reveals is the importance of diverse and redundant safety systems. The MITR design features numerous safety systems all meant to limit the dose to the public. Firstly, the MITR has two different routes to shutdown, one by dropping shim blades and the other by dumping the heavy water reflector. Both of these shutdown mechanisms are fail-safe in regard to loss of power, and thus would both need to be defeated by an attacking force in order to carry out acts of sabotage. This is different than the Aurora design, which has redundant safety in the form of three shutdown rods when only one is needed to shut the reactor down. However, this is the only type of shutdown system that the design employs, and as such may make it easier for an attacking force to prevent shutdown. MITR also features a full containment, to act as a final layer of defense in depth for preventing and mitigating doses to the public. This was likely the key factor in the orders of magnitude difference between the predicted doses of the Aurora versus the MITR.

5.1.3 General Conclusions

The consequence analysis of two different reactors designed and built decades apart revealed a few important general conclusions that should be considered looking ahead to future work and applications. Firstly, between the MITR design and the Aurora

design, the growing trend towards simplicity in advanced fission reactors is illustrated. The Aurora design is very simple in comparison to the MITR, having fewer structures, systems and components overall. This simplicity is a good reason to use the consequence-based analysis, since pathways and consequences can be easily identified. The simplicity helps to limit the possible types of attacks, which limits the number of pathways, thus allowing a more focused approach to security.

Both the MITR and Aurora designs utilized some form of automatic shutdown. In both consequence analyses, using parameter interlocks for automatic shutdown was identified as a potential pathway to radiological sabotage. It is highly likely that other micro-reactor designs intend to be at least partially, if not fully, automated and operate without dedicated reactor operators. As such, protection of the reactor trip setpoints is a major concern for micro-reactor physical security. There could be numerous ways to protect these reactor setpoints, including physical controls and administrative controls. The physical controls could be to have the logic cabinets (which store the reactor trip logic systems) incorporate delay mechanisms, such as custom locks, special barriers, sticky foam, slippery surfaces, or fog. If these mechanisms can delay an attacking force long enough for an offsite response force to arrive before setpoints are sabotaged, the consequences could be prevented. Another type of physical control of these setpoints could be to eliminate the possibility to reprogram the setpoints onsite, but rather have the entire micro-reactor programmed in its manufacturing facility, and require that the system must be sent back for any changes to these setpoints. Administrative controls could also be used, such as the use of offsite authorization for certain onsite tasks. This authorization could include requiring passcodes that are updated frequently, or using some form of two-factor authentication such as needing a button or switch both onsite and offsite to be engaged in order to allow changes.

5.2 Improvements and Future Work

The consequence-based methodology should be expanded to include other micro-reactor designs, and take the further step to begin recommending solutions to common problems. This analysis included a light-water cooled design as well as a heat pipe cooled design. Other potential micro-reactor designs include high-temperature gas reactors, sodium fast reactors, lead fast reactors, and molten salt reactors. A design from each of these classes of reactors should be analyzed using the consequence approach, and from there general conclusions about micro-reactors can be drawn. Additionally, these analyses would be improved with more in-depth worst-case scenario dose consequence analyses. This would require more data beyond what is included in the FSAR for a proposed design, and thus studies would need to work more directly with designers to make more accurate dose predictions. Once more consequences analyses have been done, with more accurate dose calculations, general guidance could be provided to alert reactor designers and owners to important security concerns that must be protected against. Recommendations for proposed solutions to these concerns could also be adapted for a generic site, thus generating basic models for onsite physical security at micro-reactors.

Appendix A

Formal Consequence Analysis

A.1 Analysis Format

For each concern, a formal consequence analysis is explained. The format for each concern is to first identify the potential pathways to the concern, including the potential targets. Next, the analysis enumerates the plant's mitigation features, in the form of inherent features, engineered features and/or plant layout, and human intervention. Considering the potential pathways and the mitigation features, it is determined if the concern is credible and if an attacker can feasibly produce that outcome. If this is true, and the concern is credible, the dose consequences are reported. Lastly, the timeframe of the concern is considered, both from the attacker perspective and the plant perspective. As previously stated, this would help future work in determining the goals of added physical protection systems; how much delay they would need to cause to allow proper time for onsite or offsite response.

The consequence analyses for each concern for both the MITR and the Aurora follow the above format.

A.2 Oklo Aurora Consequence Analyses

Concern: Theft of Radioactive Materials

Potential Pathway to Consequence

1. Fixed crane onsite, housed in Power Conversion System area on the ground floor of the powerhouse building, normally used to load and unload the reactor through a door in the ground level floor, could be used to steal the entire reactor unit. Reactor small enough to be transported as a whole on the bed of a large truck.

2. Individual reactor cells (114 in core) can be stolen via the forced assistance of Onsite Monitors, where the Onsite Monitors, used as hostages, remove the fuel from the core and carry it to the attackers' vehicles for transportation from the site.

Mitigation Features

Inherent Plant Features

- No spent fuel storage onsite, limiting the target set to in-core fuel only, and total fuel of Aurora (5 metric tons) is only 5% of total fuel of a typical large light water reactor (LWR), making the overall site less attractive than current LWRs.

- Fuel form is an annular fuel matrix, not fuel rods or fuel pellets, adding difficulty to the physical separation of fuel from the reactor cell.

- In-core fuel highly radioactive and inherently self-protecting, would harm an individual attempting to steal unshielded reactor cells (why the pathway is assumed to be hostages handling the fuel rather than attackers).

Physical Layout

- Reactor is anchored to the basement floor, adding difficulty to removing the reactor as a whole unit.

- Three boundaries between fuel and powerhouse basement; reactor cell contained in steel envelope, entire core array contained in steel capsule, and overall reactor housed in steel vessel; difficult to remove individual reactor cells.

Fuel Reprocessing

- Fuel itself would require sophisticated processing techniques and equipment to be made into a form usable in a nuclear weapon.

Consequence

- Theft of in-core fuel has potential off-site consequences in the form of nuclear devices.
- Fuel used in the Aurora is 19.75% enriched, while not weapon-grade, it could be a possible feed material for enrichment to nuclear weapon grade, but more easily a source for a radiological dispersal device (dirty bomb) or radiological exposure device. Irradiated fuel would need further enrichment to become a nuclear weapon, but no sophisticated processing to be used as an exposure device or dirty bomb, thus these are more likely consequences.

Time Interval

Attack Timeframe

- Removal of whole reactor or individual reactor cells would likely take on the order of an hour or more.

Plant Workers' Response Timeframe

- Security events are classified as unusual events, and must be declared by Onsite Monitors within 15 minutes. Declaration would trigger offsite security team to dispatch to the site.
- If material is successfully stolen, law enforcement is likely to track and attempt recapture as soon as possible, thus preventing severe consequences of any future weapon made from stolen materials.

Concern: Theft or Manipulation of Sensitive Nuclear Information

Potential Pathway to Consequence

1. One-way, outgoing communication from Aurora reactor's intrusion detection system and security video surveillance (inside and outside powerhouse building) goes to offsite computers at Oklo Power Headquarters and the supporting contracted security headquarters. This stream could be monitored or even cut-off by an adversary. Connection could also be manipulated by adversary to stream "false positive" data; broadcasting data that the plant is in a safe state when it is not.

2. Important security information could also be obtained through direct download at the Aurora site, Oklo Power Headquarters, or the supporting contracted security headquarters.

Mitigation Features

- No specific information protection mechanisms have been described in the FSAR, but Oklo presumably has plans to implement cybersecurity.

Consequence

- Theft of sensitive nuclear information can be used to plan attacks against facilities. This includes learning about surveillance and patrol intervals to understand the best times to attack; getting sensitive design or operation information to understand the best mode of attack; and other plotting mechanisms.

- Manipulation of the data stream, to broadcast false data, could allow the attacker a cover under which to attack the plant. This could cause the attack to go undetected, or at least delay the offsite response.

Time Interval

Attack Timeframe

- Desired data and information can be downloaded or monitored near instantaneously once connected to Aurora's digital computer system, or the systems at Oklo Power Headquarters or the offsite security headquarters.

Plant Workers' Response Timeframe

- If communications are interrupted, an unusual event must be declared by Onsite Monitors within 15 minutes.

Concern: Reactivity Excursion

Potential Pathway to Consequence

Description of Potential Targets

- Reactivity of the Aurora core controlled via three control drums, three shutdown rods, and a series of reflectors and absorbers. Only the control drums and shutdown rods function through active systems, and thus could be manipulated by the attacking force.

- Shutdown rods and control drums are controlled via two redundant Control Cabinets, which are housed in the Power Conversion System (PCS) area of the ground floor of the powerhouse. These Control Cabinets store the logic for reactor trips and receive data from sensors in and around the core and PCS. If data from these sources falls outside specified operating safety limits, a fault signal is generated and the reactor is automatically tripped. Only one Control Cabinet actively controls the reactor at any time; active cabinet is determined via a switch in the powerhouse building.

- Only potential source of positive reactivity insertion to the core are the control drums. These consist of half reflector, half absorber, and fully rotating the reflector of all three drums to face the core would add 700 pcm.

Potential Pathways

In each pathway, it is assumed that a reactivity insertion, via rotation of the control drum's reflector to face the core, occurs. This could be accomplished via physical forced rotation of the drums by attackers or by manipulating the automatic reactor controls that normally control the rotation, located in the Control Cabinets (likely an insider attack).

1. Operating safety limits set manually in the Control Cabinets, offering a potential source of sabotage. Changing these setpoints could cause the reactor not to trip, even in an unsafe event, such as reactor overpower. This lack of automatic trip

could allow for a reactivity excursion to proceed without scram. This attack would likely require an insider at the facility who has the knowledge of how to change the setpoints; or a hostile takeover of the plant could force Onsite Monitors to change setpoints at attackers' demand.

2. Control Cabinets could be disabled through a fire set in each space, or explosion in each space. Control Cabinets are separated by rated fire barriers, thus a fire in one cannot spread to the other, and individual fires must be set. Disabling the Control Cabinets could disable the reactor's ability to shut down.

3. Gap between active portion of shutdown rods and walls of the channel that house the rods in the core is 0.797 cm. Shutdown rods normally held just above active core via electromagnets; trip signal cuts power to electromagnets to cause drop. Forceful impediment of the shutdown rod channels, through blockages or warping of the channel from physical sabotage, could prevent the dropping of shutdown rods. Only one shutdown rod (worth $>$ 1400 pcm) required to scram the reactor, so all three shutdown rods must be disabled to prevent a scram.

Mitigation Features

Inherent Plant Features

- Criticality of Aurora achieved by secondary design features (i.e., neutron absorbers and reflectors; core geometry; etc.) that optimize and preserve neutron population, not enrichment levels or fuel quantities alone.

- Fast neutron spectrum of Aurora translates to large neutron free paths, helping to react to transients uniformly and limit the susceptibility of localized peaking events.

- Core has inherent negative reactivity feedback to temperature increase due to doppler broadening and thermal expansion of fuel and structural materials.

- Metal fuels, like the UZr in Aurora, retain most fission products within the fuel, so long as burnup is maintained below 1% atomic (Aurora intends to operate

below 1% atomic over full 20-year lifetime). UZr fuel also has high thermal conductivity to reduce peaking, and reasonably high melting point (1230°C).

- Heat pipe performance increases with temperature; good for removing heat during transients or lack of scram.
- Reactor operates near standard/atmospheric pressure, which implies no large pressure difference between core and basement interior to help drive release of fission products.

Physical Layout / Engineered Features

- No single-barrier failure will cause a release; three barriers between fuel and powerhouse basement, at least two walls between basement interior and powerhouse exterior. High thermal conductivity of the three metal barriers between fuel and basement allow for effective heat removal both radially and axially.
- Control drums programmed with rotational limit of 10^{-2} deg/sec; programmed not to go faster, unclear if that can be maliciously re-programmed. When not rotating, control drums locked in place via electromagnetic brake. Drums stop in place during a reactor trip or loss of control system (loss of Control Cabinets).
- Shutdown rods do not rely on offsite power; trip signal is the loss of power to shutdown rod electromagnets, so any power loss would cause automatic trip. Further, Aurora never uses offsite power; relies on onsite battery charged by the plant itself.

Human / Plant Worker Response

- Manual reactor trip buttons located throughout the powerhouse; Onsite Monitors can force shutdown.
- Configurable components in Control Cabinets are password protected and access controlled. Control Cabinets are set to automatically trip reactor if both cabinets are nonfunctional or bypassed.

Consequence

- If burnup rises above 1% atomic, fission gas voids interconnect and release fission gases to the Ar plenum within the reactor cell. Reactor cells sealed but not considered to be airtight; fission gases may leak out of reactor cells.

- If fuel melts, beginning at 720°C (instead of 1230°C) because of eutectic interaction between fuel and surrounding steel containment, fission products are released from the fuel to the Ar plenum.

- Worst-case scenario, all fission products released to environment outside of the powerhouse building. Results in doses as predicted by other literature:

  - Dose based on HTGR study:

    * Worker: 1,664 rem
    * Public: 3.03 rem

  - Dose based on INL micro-reactor study:

    * Worker: 3,100 rem
    * Public: 50.8 rem

  - **Produces Unacceptable Radiological Consequences**
    Under proposed 10 CFR Part 73, dose at site boundary (8.5 ft/2.6 m for Aurora) cannot exceed 25 rem total effective dose equivalent (TEDE) in 2-hour period; one of the models predicts higher dose than this

---

Time Interval

Attack Timeframe

- 5 hours to rotate control drum and fully insert reflector to core (maximum timeframe; assumes initially that absorber was fully-facing core).

Plant Response Timeframe

- Normally, reactor trip takes 10 seconds, 6 seconds for detection of unsafe levels and signaling (fault signal) to the Control Cabinets, and 4 seconds for the release and drop of the shutdown rods.
- Setpoint limits must be exceeded for more than 2 seconds to initiate fault signal
  - Control drum insertion: 36 seconds until fuel temperature reaches normal over-temperature setpoint (655°C); translates to 0.45°C fuel temperature increase per second after the insertion
  - 48 seconds to shutdown
- In the event of both control cabinets bypassed or non-functional, fault signal in 5 seconds
  - 15 seconds to shutdown

Concern: Restart the Reactor After a Scram

Potential Pathway to Consequence

1. Battery onsite stores enough energy to restart the reactor, do not rely on any offsite power source. A restart requires a Startup Operator or insider knowledge to restart the reactor post-scram.

Mitigation Features

Inherent Plant Features

- Absorber cells in core have inserts for absorbers or reflectors; these are adjusted for the initial startup of core and unclear if necessary for every restart.
- Every reactor cell has fuel of same enrichment, unlike LWRs, so there cannot be any improper fuel loading or malicious sabotage upon restart.

Human / Plant Worker Response

- Offsite Startup Operators responsible for the startup of reactor and performing startup tests; these operators are separate from Onsite Monitors.

Consequence

- Potential that upon restart, attackers then proceed with other attack, such as reactivity excursion or removal of cooling systems.

Time Interval

Attack Timeframe

- Unclear from FSAR the time needed to restart Aurora reactor.

Plant Workers' Response Timeframe

- Likely would be declared an unusual event, which would occur within 15 minutes; offsite security would be dispatched to the site.

Concern: Interrupt Heat Removal Systems

Potential Pathway to Consequence

Description of Potential Targets

- Primary cooling system of the Aurora is heat pipes, one for each reactor cell. Secondary system is a supercritical carbon dioxide (sCO_2) Rankine cycle. Ultimate heat sink is an air-cooled radiator located outside of the powerhouse building; this heat sink is used when secondary system performs a turbine bypass.

- Overcooling occurs when ultimate heat sink has an overspeed failure or fails to adjust speed with a change in ambient air temperature. Overcooling leads to fuel temperature decrease and power oscillations but is not expected to challenge the fuel.

Potential Pathways

1. Heat pipes can fail if outer wick fails, but almost impossible that all heat pipes would fail at once because each is independent for each reactor cell; only malicious attack, such as an explosion, could cause multiple failures.

2. Decrease in heat removal can be caused by turbine trip, secondary system pump trip, ultimate heat sink malfunction, secondary system safety valve actuation, or sCO_2 pipe break. The pipe break is considered to be the bounding loss of heat removal event.

3. Numerous operating setpoints can trigger reactor scram in loss of heat removal event, such as a loss of sCO_2 or a fuel overtemperature. If these operating setpoints are maliciously attacked and set much higher, reactor could be prevented from scramming before fuel melt.

Mitigation Features

Inherent Plant Features

- Events involving increase in heat removal (overcooling) not challenging to safety because of lack of moderator (unlike water in LWRs that adds positive reactivity during overcooling) and lack of strong effect on neutron population.
- Core has inherent negative reactivity feedback to temperature increase due to thermal expansion of fuel and structural materials; and doppler broadening.
- Fast neutron spectrum of Aurora translates to large neutron free paths, helping to react to transients uniformly and limit the susceptibility of localized peaking events.
- UZr fuel has high thermal conductivity to reduce peaking, and reasonably high melting point (1230°C).
- Heat pipe performance increases with temperature; good for removing heat during transients or lack of scram.
- Reactor operates near standard/atmospheric pressure, which indicates no large pressure difference between core and basement interior to help drive release of fission products.

Physical Layout / Engineered Features

- Secondary system can automatically trip the reactor if not removing enough heat. If reactor successfully trips, decay heat can be removed passively through radial conduction through tens of tons of steel containment in core, then convection to air surrounding the reactor vessel, even with the loss of the secondary system (assume convection only on the sides of the reactor).
- Single heat pipe failure does not lead to cascade failures; surrounding heat pipes can remove the additional heat (each heat pipe accounts for only about 1% of the heat transfer of the core).

- Shutdown rods do not rely on offsite power; trip signal is the loss of power to shutdown rod electromagnets, so any power loss would cause automatic trip. Further, Aurora never uses offsite power; relies on onsite battery charged by the plant itself.

- No single-barrier failure will cause a release; three barriers between fuel and powerhouse basement, at least two walls between basement interior and powerhouse exterior. High thermal conductivity of the three metal barriers between fuel and basement allow for effective heat removal both radially and axially.

Human / Plant Worker Response

- Manual reactor trip buttons located throughout the powerhouse; Onsite Monitors can force shutdown.

- Configurable components in Control Cabinets are password protected and access controlled. Control Cabinets are set to automatically trip reactor if both cabinets are nonfunctional or bypassed (via the switch described previously).

Consequence

- If fuel melts (starting at 720°C), fission products are released from fuel to Ar plenum. Reactor cells not considered to be airtight; fission gases may leak out of reactor cells.

- Worst-case scenario, all fission products released to environment outside of the powerhouse building. Results in doses as predicted by other literature:

  - Dose based on HTGR study:

    * Worker: 1,664 rem

    * Public: 3.03 rem

  - Dose based on INL micro-reactor study:

    * Worker: 3,100 rem

    - Public: 50.8 rem

  - **Produces Unacceptable Radiological Consequences**
    Under proposed 10 CFR Part 73, dose at site boundary (8.5 ft/2.6 m for Aurora) cannot exceed 25 rem total effective dose equivalent (TEDE) in 2-hour period; one of the models predicts higher dose than this.

Time Interval

Attack Timeframe

- Interruption of heat removal system can be instantaneous, depending on how equipment is damaged; would take attacker a few minutes to get to equipment they desire to attack.

Plant Response Timeframe

- Reactor must be in hot standby (reactor subcritical; fuel temperature decreasing to ambient temperature) within one hour of loss of heat sink to prevent fuel melting.
- Normally, reactor trip takes 10 seconds, 6 seconds for detection of unsafe levels and signaling to the Control Cabinets, and 4 seconds for the release and drop of the shutdown rods
- Setpoint limits must be exceeded for more than 2 seconds to initiate fault signal
  - Upon loss of heat sink (loss of Power Conversion System), 20 seconds to reach fuel over-temperature setpoint; translates to 0.81°C fuel temperature increase per second after the loss of heat sink
  - 32 seconds to shutdown
- In the event of both Control Cabinets bypassed or non-functional, trip triggered in 5 seconds.
  - 15 seconds to shutdown

Concern: Breach Containment Shell with Explosives

Potential Pathway to Consequence

1. Airgap between outer containment and basement floor, to allow for passive decay heat removal; best target for breaching containment and causing release of radionuclides from the core.

2. Additional targets include Control Cabinets (to prevent a reactor trip), secondary sCO_2 system (to cause loss of heat removal), and module equipment housing, which house the electromagnets that control shutdown rods (to prevent a reactor trip).

Mitigation Features

Physical Layout / Engineered Features

- 3 steel barriers between airgap and fuel; must all be breached to allow radionuclide release.

- Blast hazard analysis done for the general site envelope; collapse of powerhouse building and crane onto reactor does not cause safety concern.

- Module equipment housing has calculated ultimate tensile strength of 517 MPa (withstands powerhouse building collapse, so shutdown can still occur in that scenario).

Consequence

- Worst-case scenario, all fission products released to environment outside of the powerhouse building. Results in doses as predicted by other literature:
  - Dose based on HTGR study:
    - Worker: 1,664 rem
    - Public: 3.03 rem

- Dose based on INL micro-reactor study:
  - Worker: 3,100 rem
  - Public: 50.8 rem
- **Produces Unacceptable Radiological Consequences**
  Under proposed 10 CFR Part 73, dose at site boundary (8.5 ft/2.6 m for Aurora) cannot exceed 25 rem total effective dose equivalent (TEDE) in 2-hour period; one of the models predicts higher dose than this.

Time Interval

Attack Timeframe

- Explosion near instantaneous; would require a few minutes to get to powerhouse building basement to attack containment.

Plant Workers' Response Timeframe

- Emergencies onsite must be declared within 15 minutes of initial observation; offsite response would be dispatched to the site.

A.3 MITR Consequence Analyses

Concern: Theft of Radioactive Material

Potential Pathway to Consequence

Description of Potential Targets

- MITR core tank houses active fuel, in the form of up to 27 fuel elements, each containing 15 fuel plates.
- New fuel can be stored in the core, in the cadmium-lined fuel storage ring attached to the flow shroud, or in the storage safe in the containment building.
- Irradiated fuel can also be stored in the fuel storage ring in the core, in the spent fuel pool in the containment building basement, in the fission converter tank outside the graphite reflector, or in fuel element transfer casks in controlled areas.
- MITR is also licensed to have an onsite non-reactor source inventory of up to 100,000 Ci (1,000 Ci max for any one sample, max dose rate unshielded at 1 meter: 100 rad/h). Sources may be stored in the hot cell area or shielded wall storage, both located on the ground floor of the containment building.
- Tritium produced in the heavy water (D_2O) reflector may also be a target. However, given that the material is in liquid form, and the maximum allowable tritium concentration in the heavy water tank is controlled at 5 Ci/L, this is an unlikely target.

Potential Pathways

1. Fixed polar crane located inside containment can be used to access materials in the core tank, the spent fuel pool, and the hot cell area. Once removed from core tank, fuel elements (fresh, active, or irradiated) could be transported away from site via truck airlock located on ground floor of containment building. Pathway

likely requires insider knowledge or the forced assistance of reactor operator to operate polar crane. Forced assistance of reactor operators and other onsite personnel likely to be used to handle the fuel elements outside of the core and load them onto attackers' vehicle.

Mitigation Features

Inherent Plant Features

- Active and irradiated fuel highly radioactive and inherently self-protecting for multiple years; plant workers and adversaries would be open to the risk of radiation exposure if they handle unshielded fuel elements.

Physical Layout / Engineered Features

- To remove fuel from the core tank, hold-down grid must be disengaged, then use the crane and basket attachment to remove fuel elements. Interlocks prevent the top hold-down grid from being unlatched without a reactor shutdown; all shim blades must be inserted and the coolant pumps shut off for the hold-down grid to be unlatched. Further, unlatching the grid causes a scram signal, so if the reactor were not fully shutdown, it would be shutdown.

Fuel Reprocessing

- Fuel itself would require sophisticated chemical processing techniques and equipment to be made into a form usable in a nuclear weapon.

Consequence

- Theft of fuel or other radioactive materials has potential off-site consequences in the form of nuclear devices.

- Fuel used in the MITR is highly enriched ($>$ 20% ^{235}U enrichment), making it a possible feed material for nuclear weapon development, but more easily a source for a radiological dispersal device (dirty bomb) or radiological exposure

device. Fuel would need sophisticated processing to become a nuclear weapon, but not as much to be used as an exposure device or dirty bomb. Additionally, non-fuel radioactive materials can be used for exposure devices or dirty bombs, thus these are more sources available for these devices.

Time Interval

Attack Timeframe

- Removal of fuel from containment would likely take on the order of an hour or more.

Plant Workers' Response Timeframe

- If material is successfully stolen, law enforcement likely to track and attempt recapture as soon as possible, thus preventing severe consequences of any future weapon made from stolen materials.

Concern: Reactivity Excursion

Potential Pathway to Consequence

Description of Potential Targets

- Reactivity of the MITR core controlled via six shim blades, one regulating rod, heavy water reflector, graphite reflector, and other fixed absorbers.
- Shim blades and regulating rod are controlled via control room manual controls. During normal operation, the regulating rod can be placed in automatic mode, where the rod is moved via logic systems to maintain a specific power level. The rod can be returned to manual operation by moving the control switch for the regulating rod.
- Boron stainless steel fixed absorbers ensure an appropriate shape of the neutron flux for experiments under the core.
- Heavy water (D_2O) tank surrounds the central core tank and has substantial reactivity worth. Dumping the D_2O reflector renders the core subcritical, even without control blades inserted.
- Potential sources of positive reactivity insertion to the core include the shim blades and regulating rod. Shim blades are worth approximately 2 beta (1600 pcm) each (total worth of all 6: 12.63 beta/9600 pcm); the regulating rod is worth about 0.16 beta (160 pcm). Other factors including pump-up, core temperature decrease, experiments and sample reactivity, etc. all can contribute to reactivity changes.

Potential Pathways

The reactor protection system monitors reactor power, period, coolant outlet temp, coolant flow and core tank level. This system uses coincidence logic, i.e., system will generate a scram signal if instruments monitoring these reactor parameters detect an unsafe reading (signal reading falls outside setpoints). MITR has 3 types of shutdown:

a minor scram, which drops all shim blades; a major scram, which drops all shim blades, dumps the D_2O reflector and isolates the containment building; and a dump of the D_2O reflector alone, which can shutdown the reactor without shim blade drop.

1. Shim blades may be manually operated to insert positive reactivity into the core. The withdrawal of shim blades would increase the reactivity in the core. To cause damage, the reactor would need to be prevented from scram during the insertion of positive reactivity. This could be done by changing the scram setpoint values or by preventing the drop of at least 2 shim blades (only 5 shim blades required to operate and shutdown MITR). The shim blades could be prevented from dropping via explosion or other forceful prevention, since each shim blade has its own electromagnet and drive mechanism.

Mitigation Features

Inherent Plant Features

- Core is intentionally under-moderated, helping to limit damage from reactivity excursions.
- Both the fuel and light water moderator have negative reactivity coefficients with respect to temperature increase. Light water coolant also has negative void coefficient of reactivity.
- Leak-tight full containment helps retain any fission product buildup within the reactor building, limiting exposure to environment. Containment interior pressure slightly below atmospheric to prevent leak-out of any fission products.
- Fuel plates have finned surfaces which increase heat transfer, helping to prevent fuel degradation and fission product release from fuel.
- Mixing of light water core tank with D_2O reflector tank results in negative reactivity insertion to the core due to decreased moderation and increased neutron absorption.

- MITR core is critical at shim blade height of between 7-9 inches, meaning each shim blade would need to be withdrawn 12-14 inches to insert their full 2 beta (1600 pcm) worth.

Physical Layout / Engineered Features

- Shim blades are held up via electromagnets and scram occurs by cutting power to electromagnets to drop the blades. Thus, blades drop for any loss of power. Also, on loss of power, D_2O reflector dumps and the containment building is isolated.

- Containment isolation system prevents release of fission products. Exhaust ventilation from the containment building flows through the holdup plenum; radiation monitors at entrance to the plenum trigger dampers at the exit to close if there are high levels of radiation. Dampers at exit and entrance of plenum close and seal the plenum to prevent release to the environment or back to the containment. There are 2 redundant damper systems, a main system controlled hydraulically, and an auxiliary system controlled by gravity that close if the main dampers take too long to close. Both sets of dampers close automatically on loss of power.

- D_2O reflector also dumps with a loss of compressed air, or manually via 2 different buttons in the control room. The reflector can still dump even if there is mixing of the light water core tank and reflector tank; fuel will not be uncovered.

- Shim blades are always aligned with blade slot because the range of travel for each blade prevents it from ever fully exiting its guide slot.

- Shim blades move 4.25 inches per minute and only one shim blade can be withdrawn at one time.

- Fuel is a cermet UAlx fuel sealed in Al cladding, and is sintered to have a specific void fraction (4-7%). This void helps to retain fission gas products in the fuel itself.

- Containment pressure relief system is used to maintain sub-atmospheric pressure in containment building once containment is isolated. This system is manually activated and can be initiated from outside containment. Processes and removes radioactive particulates from containment air before vented release to the environment. Processing focuses on Iodine; releases 100% of noble gases and Br, less than 1% I, 50% all other fission products.

- If there is an overpressure in the containment building, leak rate of 1% of building volume per day per psi of overpressure.

Human / Plant Worker Response

- Manual reactor trip buttons located in multiple places onsite, so reactor operators can force shutdown.

Consequence

- FSAR states that from testing, it is known that:
  - 3 beta (2400 pcm) step insertion during forced convection results in 360°C clad temperature.
  - 2 beta (1600 pcm) step insertion during natural convection results in 531°C clad temperature; higher temperature because low power and low temperature of core means low feedback effects to protect against temperature rise.

- If fuel melts (using Al clad softening point of 450°C as a conservative estimate of the beginning of melting) fission products retained in the voids in the fuel would be released.

- MITR FSAR maximum hypothetical accident, which assumes the entire active portion of 4 fuel plates melt (4/360 plates in core) results in a maximum whole-body dose in 2 hours at the site boundary of 247 mrem.

- For worst-case, all fuel plates melt, results in 22.23 rem TEDE at site boundary
- **Does NOT Produce Unacceptable Radiological Consequences** Under proposed 10 CFR Part 73, dose at site boundary (8-21 meters for MITR) cannot exceed 25 rem total effective dose equivalent (TEDE) in 2-hour period; does not exceed.

Time Interval

Attack Timeframe

- Takes approximately 3 minutes to fully withdraw one shim blade; thus about 18 minutes to withdraw all 6 shim blades.

Plant Workers' Response Timeframe

- Time from initiation of scram signal for shim blade to go from full-out to 80% inserted is less than one second.

Concern: Restart the Reactor After a Scram

Potential Pathway to Consequence

1. Manual controls in control room can be used to restart reactor. Startups are normally performed by reactor operators.

Mitigation Features

Physical Layout / Engineered Features

- Must have console key to be able to start up reactor; without the key the reactor is in a secured state and nothing can be done.
- Subcritical interlock helps to prevent rapid restart; if the reactor attains criticality at a shim bank height of less than 5 inches then the reactor must be shutdown and startup cannot proceed.
  - However, this interlock can be bypassed by pulling and holding the "subcritical-bypass" lever while the shim blade control switch is manipulated.
- During startup, must move each shim blade one at a time while maintaining bank height, and all shim blades must reach 4” before any blade can go above this. Non-uniform bank height is then allowed above 1kW.

Human / Plant Worker Response

- Manual reactor trip buttons located in multiple places onsite, so reactor operators can force shutdown.

Consequence

- Potential that upon restart, attackers then proceed with other attack, such as reactivity excursion or removal of cooling systems.

Time Interval

Attack Timeframe

- Time needed to restart MITR reactor ranges from 1-6 hours.

Concern: Interrupt Heat Removal Systems

Potential Pathway to Consequence

Description of Potential Targets

- Primary cooling system of the MITR is a closed light water loop. This loop, combined with cooling loops in the heavy water (D_2O) reflector and thermal shield system, transfers heat produced in the core to the secondary cycle.
- Light water secondary cycle rejects heat via cooling towers, which can reject 10 MW through forced convection.
- D_2O reflector system has its own heat exchanger to transfer heat to the secondary system.
- Thermal shield, made of lead and steel and located outside of the graphite reflector, uses 2 sets of redundant coil systems filled with demineralized water plus a heat exchanger to transfer heat to the secondary system.
- Coolant pumps for all systems are housed in the containment basement equipment room.

Potential Pathways

1. Simultaneous rupture of core and D_2O reflector tanks, likely via an explosion in or near the core tank.
2. Simultaneous rupture of core tank inlet pipe and failure or compromise of both anti-siphon valves.
3. Core tank puncture below anti-siphon valves.

Mitigation Features

Inherent Plant Features

- MITR core is housed in 2 concentric tanks, the light water core tank surrounded by the D_2O reflector tank. Both would need to rupture to cause fuel to become uncovered.

- Leak-tight full containment helps retain any fission product buildup within the reactor building, limiting exposure to environment. Containment interior slightly below atmospheric pressure to prevent leak-out of any fission products.

- Fuel plates have finned surfaces which increase heat transfer, helping to prevent fuel degradation and fission product release from fuel.

Physical Layout / Engineered Features

- Reactor automatically scrams in the event of low flow in the primary cooling system or in the D_2O reflector system. Scram also occurs if core tank level falls below set limit.

- Inlet piping to core all above core and anti-siphon valves, allowing valves to work properly. Anti-siphon valves isolate the core tank from effects of coolant piping breaks, by ensuring that the water in the core tank does not flow out of the tank, but rather begins to circulate through the core without forced flow. This circulation is driven by natural convection through the core.

- Natural circulation valves offer an additional path to natural convection in the core. Natural convection can remove up to 100 kW of heat from the core, so reactor must be shut down or at low power, and this system can remove decay heat without a functioning secondary system.

- Only need 3 natural circulation valves or 1 anti-siphon valve to establish natural convection in the core. Both types of valves open whenever there is no forced flow.

- Even if D_2O reflector dumped, natural convection in the core still possible.

- Emergency Core Cooling System (ECCS) sprays water onto the core at a rate sufficient to remove decay heat. ECCS has two redundant nozzle systems and must be initiated manually. The ECCS can be initiated from outside the containment building.

- Capability to provide normal shutdown cooling does not require electricity; during normal operation, the heat exchangers are cooled via the secondary system, but in loss of power one of the core tank's heat exchangers can instead be cooled by city water.

- Shim blades are held up via electromagnets and scram occurs by cutting power to electromagnets to drop the blades. Thus, blades drop for any loss of power. Also, on loss of power, D_2O reflector dumps and the containment building is isolated.

- Containment isolation system prevents release of fission products. Exhaust ventilation from the containment building flows through the holdup plenum; radiation monitors at entrance to the plenum trigger dampers at the exit to close if there are high levels of radiation. Dampers at exit and entrance of plenum close and seal the plenum to prevent release to the environment or back to the containment. There are 2 redundant damper systems, a main system controlled hydraulically, and an auxiliary system controlled by gravity that close if the main dampers take too long to close. Both sets of dampers close automatically on loss of power.

- D_2O reflector also dumps with a loss of compressed air, or manually via 2 different buttons in the control room. The reflector can still dump even if there is mixing of the light water core tank and reflector tank; fuel will not be uncovered.

- Shim blades are always aligned with blade slot because the range of travel for each blade prevents it from ever fully exiting its guide slot.

- Fuel is a cermet UAlx fuel sealed in Al cladding, and is sintered to have a specific void fraction (4-7%). This void helps to retain fission gas products in the fuel itself.

- Containment pressure relief system is used to maintain sub-atmospheric pressure in containment building once containment is isolated. This system is manually activated and can be initiated from outside containment. Processes and removes radioactive particulates from containment air before vented release to the environment. Processing focuses on Iodine; releases 100% of noble gases and Br, less than 1% of I, 50% all other fission products.

- If there is an overpressure in the containment building, leak rate of 1% of building volume per day per psi of overpressure.

Human / Plant Worker Response

- Manual reactor trip buttons located in multiple places onsite, so reactor operators can force shutdown.

Consequence

- If cooling of the thermal shield is interrupted, the shield could melt.

- If cooling of the D_2O reflector is interrupted, the excess heat in the core could cause boiling of primary coolant.

- If fuel melts (using Al clad softening point of 450 °C as a conservative estimate of the beginning of melting) fission products retained in the voids in the fuel would be released.

- MITR FSAR maximum hypothetical accident, which assumes the entire active portion of 4 fuel plates melt (4/360 plates in core) results in a maximum whole-body dose in 2 hours at the site boundary of 247 mrem.

  - For worst-case, all fuel plates melt, results in 22.23 rem TEDE at site boundary

- **Does NOT Produce Unacceptable Radiological Consequences**
  Under proposed 10 CFR Part 73, dose at site boundary (8-21 meters for MITR) cannot exceed 25 rem total effective dose equivalent (TEDE) in 2-hour period; does not exceed.

Time Interval

Attack Timeframe

- Interruption of the heat removal system can be instantaneous, depending on how equipment is damaged; would take attacker a few minutes to get to equipment they desire to attack.

Plant Response Timeframe

- Time from initiation of scram signal for shim blade to go from full-out to 80% inserted is less than one second.
- Takes about 7 minutes to drain core tank with a 2.5-inch break.

Concern: Breach Containment Shell with Explosives

Potential Pathway to Consequence

1. Top core tank shield lid has several penetration holes (with diameters ranging from about 3-inches to 16-inches); if uncovered would allow a space to detonate explosives.

2. Pneumatic tube system could be used to send explosives near the core before detonating them. Explosives are limited to 1-inch inner diameter. The tube system terminates in a horizontal re-entrant thimble in the graphite reflector.

Mitigation Features

Physical Layout / Engineered Features

- Containment isolation system prevents release of fission products. Exhaust ventilation from the containment building flows through the holdup plenum; radiation monitors at entrance to the plenum trigger dampers at the exit to close if there are high levels of radiation. Dampers at exit and entrance of plenum close and seal the plenum to prevent release to the environment or back to the containment. There are 2 redundant damper systems, a main system controlled hydraulically, and an auxiliary system controlled by gravity that close if the main dampers take too long to close. Both sets of dampers close automatically on loss of power.

- Containment pressure relief system is used to maintain sub-atmospheric pressure in containment building once containment is isolated. This system is manually activated and can be initiated from outside containment. Processes and removes radioactive particulates from containment air before vented release to the environment. Processing focuses on Iodine; releases 100% of noble gases and Br, less than 1% of I, 50% all other fission products.

- If there is an overpressure in the containment building, leak rate of 1% of building volume per day per psi of overpressure.

- Reactor control devices are fail-safe in event of fire and loss of power, scram can still proceed.
- Core tank designed for 60 psig; has a yield strength of 9500 psia.
- Heavy water reflector tank designed for 40 psig.

Consequence

- Containment can withstand internal pressure of 1.3×10^4 Pa greater than atmospheric pressure and 690 Pa below atmospheric pressure, otherwise containment may be compromised and no longer leak-tight.
- If fuel melts (using Al clad softening point of 450°C as a conservative estimate of the beginning of melting) fission products retained in the voids in the fuel would be released.
- MITR FSAR maximum hypothetical accident, which assumes the entire active portion of 4 fuel plates melt (4/360 plates in core) results in a maximum whole-body dose in 2 hours at the site boundary of 247 mrem.
  - For worst-case, all fuel plates melt, results in 22.23 rem TEDE at site boundary
  - **Does NOT Produce Unacceptable Radiological Consequences** Under proposed 10 CFR Part 73, dose at site boundary (8-21 meters for MITR) cannot exceed 25 rem total effective dose equivalent (TEDE) in 2-hour period; does not exceed.

Time Interval

Attack Timeframe

- Explosion near instantaneous; would require more than ten minutes to get to reactor top and get set up to attack the reactor core.

Appendix B

Dose Calculations

B.1 Oklo Aurora Dose Calculations

B.1.1 Dose Based on Modular High Temperature Gas Reactor Study

The data reported in the modular high temperature gas reactor study were source terms for a 600 MW_{th} high temperature gas reactor. [43] Thus the first step in the dose calculation was to scale this source term by thermal power, dividing each source term by 600 to get an activity per MW_{th}. This data was then multiplied by 4, to scale the source term to the 4 MW_{th} size of the Aurora plant. Next, the activity was converted from units of Curie (Ci) to units of Becquerel (Bq) (using the conversion 1 Ci = 3.7×10^{10} Bq), before being multiplied by dose conversion factors. These dose conversion factors were pulled from an International Commission on Radiological Protection (ICRP) publication, and include separate factors for dose to onsite workers versus dose to the public. [45] These conversion factors were given as a cumulative dose for one person, either a worker or a member of the public, over a given time period. For the workers, this was a dose for an 8-hour shift and for a member of the public this was an annual dose. Given this, once the final scaled source term (in Bq) was multiplied by each given dose factor, the cumulative doses were converted from Sievert (Sv) to Roentgen Equivalent Man (rem) (using the conversion 1 Sv = 100

Dose Consequences From MHTGR Study		
	^{131}I	**^{137}Cs**
Source Terms from MHTGR Study	Short term: 0.61 Ci Long Term: 22.4 Ci Total: 23.01 Ci	Short term: 1.33 Ci Long Term: 1.22 Ci Total: 2.61 Ci
Total Source Terms per MW$_{th}$	0.038 Ci/MW	0.0044 Ci/MW
Source Terms for Oklo Aurora	0.15 Ci 5.66 $\times 10^{9}$ Bq	0.017 Ci 6.44 $\times 10^{8}$ Bq
Dose Factors From ICRP **• Worker** **• Public**	 1.1 $\times 10^{-8}$ Sv/Bq/8 hours 2.2 $\times 10^{-8}$ Sv/Bq/year	 6.7 $\times 10^{-9}$ Sv/Bq/8 hours 1.3 $\times 10^{-8}$ Sv/Bq/year
Worker Doses	62.3 Sv/8 hours 15.58 Sv/2 hours 1558 rem/2 hours	4.31 Sv/8 hours 1.078 Sv/2 hours 107.8 rem/2 hours
Public Doses	124.6 Sv/year 0.0284 Sv/2 hours 2.84 rem/2 hours	8.36 Sv/year 0.0019 Sv/2 hours 0.19 rem/2 hours
Total Dose at Site Boundary (I + Cs) **• Worker** **• Public**	 1664 rem/2 hours 3.03 rem/2 hours	

Table B.1: Oklo Aurora Dose Calculation

rem), then scaled for time. For workers, the cumulative does was divided by 4 to get the dose in a 2-hour period. For the public, the dose was divided by 4380 (4380 = 365 days $\times$ 24 hours per day $\div$ 2 hour interval) to get the dose in a two-hour period. This calculation is summarized in Table B.1.

B.1.2 Dose Based on INL Microreactor Study

For the molten salt micro-reactor study, the total dose presented in the report, 1.55 $\times 10^{4}$ rem for workers and 2.54 $\times 10^{2}$ for the public (each per individual), was divided by 20 to get to dose per MW$_{th}$, since the study predicted doses for a 20 MW$_{th}$ micro-reactor. [44] This dose per MW$_{th}$ was then multiplied by 4 to get the total dose for the Oklo Aurora plant. This total dose was 3,100 rem for workers and 50.8 rem for the public.

B.2 MITR Dose Calculations

To estimate the magnitude of this release, the given release for the MHA is scaled for a full-core melt. This is done by dividing the MHA release by four to get the release per plate, then multiplying by the number of plates in the core (360): [2]

$$[\text{MHA dose}] \div [\#\text{ plates melted during MHA}] \times [\#\text{ fuel elements used in normal operation}] \times [\#\text{ fuel plates per fuel element}]$$

$$247 \text{ mrem} \div 4 \times 24 \times 15 = 22.23 \text{ rem}$$

Bibliography

[1] Oklo Final Safety Analysis Report; ML20075A003. 2020. https://www.nrc.gov/docs/ML2007/ML20075A003.pdf.

[2] MIT Research Reactor Safety Analysis Report; ML053190384. February 10, 2000. https://www.nrc.gov/docs/ML0531/ML053190384.pdf.

[3] NRC Staff. 10 CFR Part 73; 38 FR 35430. December 28, 1973. https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/full-text.html.

[4] Prevent, Counter, and Respond- NNSA's Plan to Reduce Global Nuclear Threats FY 2020-FY2024. July 2019. https://www.energy.gov/sites/prod/files/2019/07/f65/FY2020_NPCR.pdf.

[5] US Department of Homeland Security. Nuclear Reactors, Materials, and Waste Sector-Specific Plan. 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-nuclear-2015-508.pdf.

[6] Mark Holt and Anthony Andrews. Nuclear Power Plant Security and Vulnerabilities. January 3, 2014. https://fas.org/sgp/crs/homesec/RL34331.pdf.

[7] Ensuring The Future of US Nuclear Energy: Creating A Streamlined And Predictable Licensing Pathway To Deployment; ML18030A771. January 23, 2018. https://www.nrc.gov/docs/ML1803/ML18030A771.pdf.

[8] Jared Conway, Neil Todreas, John Halsema, Chris Guryan, Arthur Birch, Tom Isdanavich, Jason Florek, Jacopo Buongiorno, and Michael Golay. Physical Security Analysis and Simulation of the Multi-layer Security System for the Offshore Nuclear Plant (ONP). 352. October 1, 2019. https://doi.org/10.1016/j.nucengdes.2019.110160.

[9] Tae Ho Woo. Systems Thinking Safety Analysis: Nuclear Security Assessment of Physical Protection System in Nuclear Power Plants. 2013. January 1, 2013. https://doaj.org/article/89c4be92f7034211b8e72a9ff54d494d.

[10] Hosik Yoo. A New Physical Protection Measure for Evaluating Risks at Nuclear Facilities. 36(9). September 1, 2009. https://doi.org/10.1016/j.anucene.2009.06.014.

[11] Bowen Zou, Ming Yang, Jia Guo, Junbo Wang, Emi-Reynolds Benjamin, Hang Liu, and Wei Li. Insider Threats of Physical Protection Systems in Nuclear Power Plants: Prevention and Evaluation. 104. April 1, 2018. https://doi.org/10.1016/j.pnucene.2017.08.006.

[12] NEI. Micro-Reactor Regulatory Issues. November 13, 2019. https://www.nei.org/CorporateSite/media/filefolder/resources/reports-and-briefs/NEI-White-Paper-Micro-Reactor-Regulatory-Issues.pdf.

[13] Alan Evans and Mancel Parks. U.S. Domestic Small Modular Reactor Security by Design. September 1, 2020. https://www.osti.gov/servlets/purl/1665935/.

[14] NRC Staff. Backgrounder on Research and Test Reactors. January 26, 2021. https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/research-reactors-bg.html.

[15] DOE Office of Nuclear Energy. What is High-Assay Low-Enriched Uranium (HALEU)? April 7, 2020. https://www.energy.gov/ne/articles/what-high-assay-low-enriched-uranium-haleu.

[16] Centrus Energy Corp. High-assay low-enriched uranium. https://www.centrusenergy.com/what-we-do/nuclear-fuel/high-assay-low-enriched-uranium/.

[17] Union of Concerned Scientists. Weapon Materials Basics. July 18, 2009. https://www.ucsusa.org/resources/weapon-materials-basics.

[18] Nuclear Threat Initiative. Uranium Enrichment. https://tutorials.nti.org/nuclear-101/uranium-enrichment/.

[19] IAEA. Engineering Safety Aspects of the Protection of Nuclear Power Plants Against Sabotage. September 14, 2016. https://www.iaea.org/publications/7574/engineering-safety-aspects-of-the-protection-of-nuclear-power-plants-against-sabotage.

[20] NRC Staff. 10 CFR Part 73 Proposed Rule; ML20182A157. September 14, 2020. https://www.nrc.gov/docs/ML2018/ML20182A157.pdf.

[21] NRC Staff. Technical, Licensing, and Potential Policy Issues for Micro-Reactors; ML20254A365. October 6, 2020. https://www.nrc.gov/docs/ML2025/ML20254A365.pdf.

[22] NRC Staff. Policy and Licensing Considerations Related To Micro-Reactors; ML20129J985. October 6, 2020. https://www.nrc.gov/docs/ML2012/ML20129J985.pdf.

[23] NRC Staff. 10 CFR Part 37—Physical Protection of Category 1 and Category 2 Quantities of Radioactive Material. March 19, 2013. https://www.nrc.gov/security/byproduct/10-cfr-part-37.html.

[24] IAEA. Categorization of Radioactive Sources. 2005. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1227_web.pdf.

[25] NRC Staff. 10 CFR Part 71— Packaging and Transportation of Radioactive Material. 60 FR 50264. September 28, 1995. https://www.nrc.gov/reading-rm/doc-collections/cfr/part071/index.html.

[26] 49 CFR - Transportation. https://www.ecfr.gov/cgi-bin/text-idx?gp=&SID=deffb092d4e486a34dd0cb606bcbc414&mc=true&tpl=/ecfrbrowse/Title49/49CIsubchapC.tpl.

[27] IATA. Dangerous Goods Regulations: IATA-Resolution 618-Attachment A. 2012. https://agashirinov.files.wordpress.com/2015/10/ekp000017565.pdf.

[28] Office for Nuclear Regulation. Classification Policy For the Civil Nuclear Industry. November 2017. https://www.onr.org.uk/documents/classification-policy.pdf.

[29] Office for Nuclear Regulation. Security Assessment Principles for the Civil Nuclear Industry. March 31, 2017. https://www.onr.org.uk/syaps/security-assessment-principles-2017.pdf.

[30] Office for Nuclear Regulation. CNC Response Force. March 2020. https://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-9.1.pdf.

[31] Office for Nuclear Regulation. Local Police Operations to Support the Dutyholder. March 2020. https://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-9.2.pdf.

[32] Office for Nuclear Regulation. Security Guard Services. March 2020. https://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-9.3.pdf.

[33] Office for Nuclear Regulation. Vulnerability Assessments. March 2020. https://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-6.4.pdf.

[34] Office for Nuclear Regulation. Categorisation for Theft. April 2020. https://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-6.1.pdf.

[35] Office for Nuclear Regulation. Categorisation for Sabotage. April 2020. https://www.onr.org.uk/operational/tech_asst_guides/cns-tast-gd-6.2.pdf.

[36] IAEA. Development, Use and Maintenance of the Design Basis Threat. September 16, 2016. https://www.iaea.org/publications/8097/development-use-and-maintenance-of-the-design-basis-threat.

[37] IAEA. Identification of Vital Areas at Nuclear Facilities. 2012. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1505_web.pdf.

[38] NRC Staff. ML20189A274. April 22, 2020. https://www.regulations.gov/document/NRC-2017-0227-0019.

[39] NRC Staff. Non-Power Production or Utilization Facilities Proposed License Renewal Rulemaking; ML16075A306. March 15, 2016. https://www.nrc.gov/docs/ML1607/ML16075A306.pdf.

[40] Oklo Emergency Plan; ML20075A011. 2020. https://www.nrc.gov/docs/ML2007/ML20075A011.pdf.

[41] Oklo Non-Applicabilities and Requested Exemptions; ML20075A006. 2020. https://www.nrc.gov/docs/ML2007/ML20075A006.pdf.

[42] Oklo Technical Specifications; ML20075A005. 2020. https://www.nrc.gov/docs/ML2007/ML20075A005.pdf.

[43] D. A. Petti, R. R. Hobbins, P. Lowry, and H. Gougar. Representative Source Terms and the Influence of Reactor Attributes on Functional Containment in Modular High-Temperature Gas-Cooled Reactors. 184(2). November 1, 2013. https://doi.org/10.13182/NT184-181.

[44] Troy P. Reiss. Evaluation of Microreactor Inhalation Dose Consequences. April 30, 2020. https://doi.org/10.2172/1616677.

[45] K. Eckerman, J. Harrison, H-G. Menzel, and C. H. Clement. ICRP Publication 119: Compendium of Dose Coefficients Based on ICRP Publication 60. 42(4). August 1, 2013. https://doi.org/10.1016/j.icrp.2013.05.003.