Center for
Advanced Nuclear
Energy Systems

Massachusetts Institute of Technology
77 Massachusetts Avenue, 24-215
Cambridge, MA 02139-4307

(617) 452-2660
canes@mit.edu
canes.mit.edu

Advanced Nuclear Power Program

A CYBERSECURITY FRAMEWORK FOR NUCLEAR MICROREACTORS

Matthew Chew and Jacopo Buongiorno

Department of Nuclear Science and Engineering
Massachusetts Institute of Technology

MIT-ANP-TR-197
June 2023

A CYBERSECURITY FRAMEWORK FOR NUCLEAR MICROREACTORS

Abstract

In the emerging field of modular microreactors (MMR), which have the potential to be deployed in high numbers across all sectors of the economy, very robust cybersecurity measures are necessary to prevent disruption of service and accidents. This study presents a structured, comprehensive, and easy-to-implement cybersecurity framework tailored explicitly for nuclear microreactors, aiming to streamline the identification and protection of high-priority systems and pre-emptively address threats during the project's design phase.

The proposed framework offers a strategy that brings all aspects of cybersecurity under a single, coherent plan. This approach allows microreactor developers to highlight network segments and use a risk management matrix to pinpoint high-priority systems at risk and determine necessary protective measures. As an example, applying the proposed methodology, it was found that the sensor zone, being a crucial component of the reactor protection system, could be subject to three critical vectors of attack and would require solutions such as encryption, data diode gateways and supply chain management to ensure a lower cybersecurity risk. Importantly, the framework is designed to be versatile, ensuring its applicability across a range of MMR designs and operational contexts.

CANES Reports

CANES PUBLICATIONS

Topical and progress reports are published under seven series:

Advances in Nuclear Energy Disciplines (ANED) Series
Advanced Nuclear Power Technology (ANP) Series
Nuclear Fuel Cycle Technology and Policy (NFC) Series
Nuclear Systems Enhanced Performance (NSP) Series
MIT Reactor Redesign (MITRR) Series
Nuclear Energy and Sustainability (NES) Series
Nuclear Space Applications (NSA) Series

Please visit our website (mit.edu/canes/) to view more publication lists.

MIT-ANP-TR-196 Paul E. Roege(MIT ANPEG), Alexander L. Schoonen(INL), James R. Case (INL), Corey L. Beebe(INL), Ryan Cumings (MIT LL), Zachary A. Collier (Collier Research Systems), **Assessment of Potential Ground Force Capability Enhancement Using Nuclear Microreactors** (August 2023).

MIT-ANP-TR-194 W. Robb Stewart and K. Shirvan (MIT), **Capital Cost Evaluation of Advanced Water-Cooled Reactor Designs With Consideration of Uncertainty and Risk** (June 2022).

MIT-ANP-TR-193 K. Shirvan (MIT), **Overnight Capital Cost of the Next AP1000** (March 2022).

MIT-ANP-TR-192 R. MacDonald and J. Parsons (MIT), **The Value of Nuclear Microreactors in Providing Heat and Electricity to Alaskan Communities** (October 2021).

MIT-ANP-TR-191 C. W. Forsberg (MIT) and A. W. Foss (INL), **Markets and Economic Requirements for Fission Batteries and Other Nuclear Systems** (March 2021).

MIT-ANP-TR-190 J. Buongiorno (MIT), **An Economic Evaluation of Micro-Reactors for the State of Washington** (January 2021).

MIT-ANP-TR-189 C. W. Forsberg (MIT), P. Sabharwall (INL)and A. Sowder (EPRI), **Separating Nuclear Reactors from the Power Block with Heat Storage:** A New Power Plant Design Paradigm (November 2020).

MIT-ANP-TR-188 X. Zhao and M. Golay, **Symptom-Based Conditional Failure Probability Estimation for Selected Structures, Systems, and Components:** Minor Milestone Report: Project on Design of Risk-Informed Autonomous Operation for Advanced Reactors DOE/EXT- DE-NE0008873 Project number: 19-17435 (July 2020).

MIT-ANP-TR-187 J. Buongiorno, K. Shirvan, E. Baglietto, C. Forsberg, M. Driscoll, W. Robb Stewart, Enrique Velez-Lopez (MIT), H. Einstein (Civil & Environmental Engineering), Iain Macdonald (ArtEZ), Kennard Johnston (Morgan State Univ.) and Go Hashimoto (Univ. of Tokyo), **Japan's Next Nuclear Energy System (JNext)** (March 2020).

MIT-ANP-TR-186 Y. Cai and M. W. Golay, **A Framework for Analyzing Nuclear Power Multiunit Accident Scenarios and Providing Accident Mitigation and Site Improvement Suggestions** (September 2019).

MIT-ANP-TR-185 C. W. Forsberg (MIT), P. Sabharwall and H. D. Gougar (INL), **Heat Storage Coupled to Generation IV Reactors for Variable Electricity from Base-load Reactors: Changing Markets, Technology, Nuclear-Renewables Integration and Synergisms with Solar Thermal Power Systems** INL/EXT-19-54909 (September 2019).

MIT-ANP-TR-184 C. W. Forsberg, **Implications of Carbon Constraints on (1) the Electricity Generation Mix For the United States, China, France and United Kingdom and (2) Future Nuclear System Requirements** (March 2019).

MIT-ANP-TR-183 C. W. Forsberg, **Fluoride-Salt-Cooled High-temperature Reactor (FHR) Temperature Control Options: Removing Decay Heat and Avoiding Salt Freezing** (January 2019).

MIT-ANP-TR-182 J. Buongiorno, N. Sepulveda and L. Rush, **White Paper: Potential Applications of the Modern Nuclear Fuel Cycle to (South) Australia** (November 2018).

MIT-ANP-TR-181 C. Forsberg and P. Sabharwall, **Heat Storage Options for Sodium, Salt and Helium Cooled Reactors to Enable Variable Electricity to the Grid and Heat to Industry with Base-Load Reactor Operations** (September 2018).

MIT-ANP-TR-180 C. W. Forsberg, et al. **Integrated FHR Technology Development Final Report: Tritium Management, Materials Testing, Salt Chemistry Control, Thermal Hydraulics and Neutronics with Associated Benchmarking** (September 2018).

MIT-ANP-TR-179 C. W. Forsberg, N. Sepulveda and K. Dawson **Implications of Carbon Constraints on Electricity Generation Mix For the United States, China, France and United Kingdom** (August 2018).

MIT-ANP-TR-178 C. W. Forsberg, N. Sepulveda and K. Dawson **Commercialization Basis for Fluoride-salt-cooled High-Temperature Reactors (FHRs): Base-load Reactor with Heat Storage for Variable Electricity and High-Temperature Heat to Industry** (August 2018).

MIT-ANP-TR-177 S.T. Lam, C. W. Forsberg, and R. Ballinger **Understanding Hydrogen/Tritium Behavior on Carbon to Predict and Control Tritium in Salt Reactors: Experiments, Modeling and Simulation** (August 2018).

MIT-ANP-TR-176 J. Conway, N. Todreas, and J. Buongiorno **Security and the Offshore Nuclear Plant (ONP): Security Simulation Testing and Analysis of the Multi-Layer Security System** (August 2018).

MIT-ANP-TR-175 P. A. Champlin, D. Petti, and J. Buongiorno **Techno-Economic Evaluation of Cross-Cutting Technologies for Cost Reduction in Nuclear Power Plants** (August 2018).

MIT-ANP-TR-174 L. T. Rush, D. Petti, and J. Buongiorno **Critical Assessment of Techniques, Markets and Overall Economics of Generation III+ and IV Reactors** (August 2018).

Acknowledgments

The first author is grateful to MIT Nuclear Science & Engineering Department, Center for Advanced Nuclear Energy Systems (CANES), for granting this opportunity to work on the term project. It is part of the efforts to develop Modular Microreactors (MMRs) for the nuclear energy industry. The author also acknowledges our sponsors for their support, which has been instrumental in the success of this project.

Additionally, thank Professor Jacopo Buongiorno for recommending this term project; and Professor Michael P. Short for his guidance and advice in joining the MIT Leader for Global Operations (LGO) program. This program allowed the first author to work as a Research Assistant and participate in the MMRs project.

The author is also thankful to Christopher M. Spirito from the Idaho National Laboratory (INL) for his valuable guidance that helped identify the appropriate risks to consider based on his experience and current work at INL. Lastly, the support and encouragement of family have been instrumental in achieving the successful completion of this term project.

Contents

1. Introduction

The nuclear industry is undergoing a transformation with new innovative reactor designs and operational models in an effort to make nuclear energy more affordable for many countries to add nuclear energy as part of their decarbonization portfolios. Small Modular Reactors (SMRs) and Micro Modular Reactors (MMRs) are the two main design paradigms many nuclear countries and companies are currently pursing.

However, SMRs and MMRs in particular operate under completely different conditions compared to traditional large gigawatt-scale nuclear reactors. While traditional reactors are built in buildings that are custom-made for a particular site, SMRs and MMRs are meant to be standardized in design so as to achieve efficient economies-of-scale with many components, even elements of the reactor building, standardized and manufactured in a central facility. In addition, SMR designs such as NuScale's VOYGR will feature up to a dozen co-located reactor cores simultaneously [1] compared to plants such as Georgia's Vogtle plant which operates only 4 independent 1GWe reactors [2], while SMRs and MMRs are being designed for not just distributed generation but remote operations [3]. Coupled with the need for more digitalization to ensure remote operations and multi-reactor core coordination, SMRs and MMRs create a whole new paradigm of challenges for cybersecurity protections in the nuclear industry.

In this work, the focus will be wholly on MMRs as SMRs, while having the challenges above, are meant to be operated in medium sized Nuclear Power Plant (NPP) facilities which bear similarities in terms of security to traditional gigawatt plant. MMRs on the other hand, with the aim of full remote operations/monitoring, will require more rigorous cybersecurity frameworks and protections.

There is not yet a framework to help analyzing MMRs cybersecurity vulnerabilities and ensuring a critical licensing requirement is met. Such a framework should be developed at the design phase. This work will attempt to define a suitable cybersecurity protection framework for MMRs.

2. Current state of cybersecurity in Nuclear

Cybersecurity in the nuclear industry is not a recent development. Since the 90s, the US Nuclear Regulatory Commission (NRC) has had a framework regarding the governance of cybersecurity for the operation of reactors [4]. While many reactors operated in the USA were built in the 60s and 70s, many of them received periodic upgrades in their computer systems over their long decades of operation. As more computer systems were put in place and as more cyberattacks were perpetrated world-wide with the widespread use of the internet, the NRC felt that a comprehensive cybersecurity framework was required.

Given the digital transformation of industrial systems, cybersecurity is no longer a peripheral concern; instead, it has become central to the safety, security, and functionality of nuclear facilities. Two key global entities in this arena are the International Atomic Energy Agency (IAEA) and the Nuclear Regulatory Commission (NRC), each with their unique policies and guidance frameworks.

The IAEA provides a detailed guidance specific to nuclear facilities, encompassing a broad range of aspects concerning computer security. Their comprehensive computer security policy outlines the objectives, scope, roles, and responsibilities pertaining to computer security within nuclear facilities. By identifying potential threats, vulnerabilities, and the consequences of these risks, the IAEA guidance helps facilities to maintain an effective risk assessment methodology, crucial to the overall cybersecurity strategy.

Moreover, organizational structure is a key component, establishing clear authority lines and accountability for computer security. One cannot overlook personnel security in this framework, as ensuring staff and contractors maintain a level of trustworthiness and competence is paramount. Physical security aids in the protection of computer-based systems from unauthorized access or damage. Technical security measures, including controls such as encryption, authentication, and firewalls, fortify these defences.

Another aspect of cybersecurity advised by IAEA is the use of single-flow communication for critical systems within nuclear reactor facilities as demonstrated in the figure below. This ensures that critical systems that perform tasks such as monitoring the parameters in the core cannot be accessed by outside and unauthorized personnel.

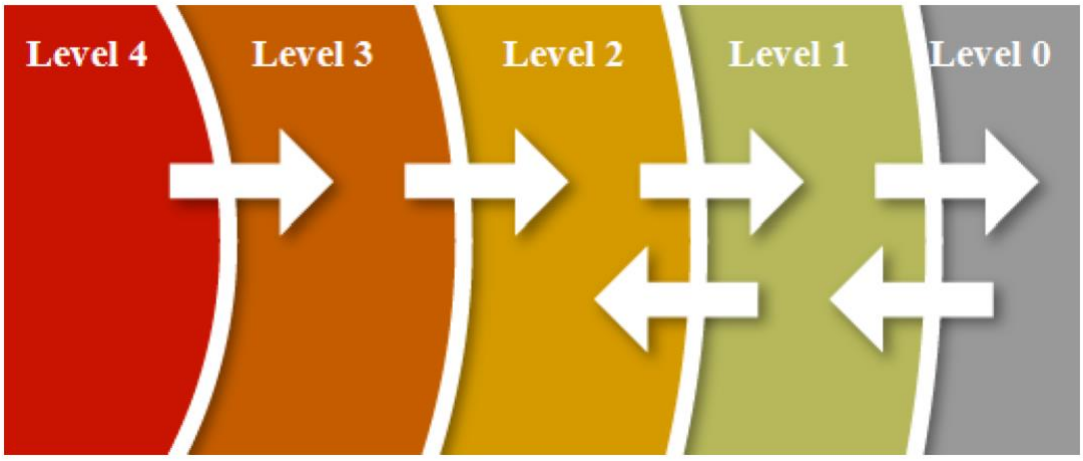

Figure 1 Recommended IAEA defense-in-depth communication pathway. These levels go from 0 – 4 with level 0 systems being the most open and non-critical to level 4 which are considered the most critical assets that relate to the safe operation of the reactor. The arrows represent pathways of communication and represents how an asset at each level may communicate. For example a Level 4 asset can only communicate down to a Level 3 asset and a Level 2 asset may only receive communication from a Level 3 asset but can have 2 way communication with a Level 1 asset.

Moreover, the IAEA promotes incident response preparedness and management to effectively handle computer security events. In tandem with incident response is contingency planning, ensuring the continuity and recovery of critical functions. Finally, auditing plays a significant role, providing a means to monitor and evaluate the performance of computer security measures. These policies collectively form a robust cybersecurity infrastructure in compliance with IAEA guidelines.

In addition to providing guidance, the IAEA also assists States in developing comprehensive computer and information security activities through training courses, workshops, peer reviews, and technical cooperation projects. These efforts enhance the skills of computer security professionals, regulators, operators, and stakeholders; sharing good practices, lessons learned, and recommendations to bolster computer security [5].

The NRC has also undertaken several actions to address cybersecurity challenges facing nuclear power plants in the US. Infrastructure changes include establishing a cybersecurity directorate within the Office of Nuclear Security and Incident Response. Enhancing interagency interfaces, the NRC has collaborated with various agencies like the Department of Homeland Security and the Federal Bureau of Investigation to bolster cybersecurity. The NRC also performs inspections and has developed a cybersecurity roadmap outlining its strategic vision and goals.

Nuclear power plant licensees are required by the NRC to implement cybersecurity plans that protect their digital systems. The NRC's regulatory framework for cybersecurity, comprising 10 CFR Part 73.54, Regulatory Guide 5.71, NEI 08-09 Rev. 6, and NUREG/CR-7117, provides a solid foundation for developing and implementing a cybersecurity plan and assessing cyber risks [6].

Furthermore, the NRC conducts inspections and assessments to verify the effectiveness of these cybersecurity programs. Through Inspection Manual Chapter 0730, Inspection Procedure 71130.08, Temporary Instruction 2201/004, and Cybersecurity Performance Indicators, the NRC ensures a comprehensive evaluation of the cybersecurity measures in place [6].

It is also important to note that the NRC and the IAEA advocate for the use of cybersecurity architectures that ensure communication is one-way. The principle of unidirectional security gateways restricts data flow to a single direction, thus preventing any potential cyber-attacks from spreading within the network.

In the next section, we will look at Micromodular Reactors (MMRs) and understand the gaps in their cybersecurity solutions and possible frameworks we could use to analyse and protect these novel systems.

2.1 Modular microreactors

Microreactors and traditional gigawatt-scale nuclear reactors or small modular reactors (SMRs) exhibit several operational differences that stem from their design, size, and intended applications, as explained next.

- Power Output and Size

Microreactors have very low power output, usually below 10 MWe, and extremely compact size, that is???. This contrasts with traditional gigawatt-scale reactors, which are large how large??? and have power outputs ranging from 600 to 1600 MWe. SMRs have physical sizes and power outputs in between those ranges.

- Mobility and Deployment:

Microreactors are designed to be transportable and rapidly deployable. Their small size and modular design allow them to be transported to and installed in remote or off-grid locations. On the other hand, large reactors and SMRs are immobile, designed to be permanently installed in a specific location.

- Fuelling and Operation Cycle:

Microreactors, depending on their specific design, can operate for several years (possibly up to 20 years) without refuelling due to their low power density and relatively high enrichment. Traditional reactors typically require refuelling every 18 to 24 months, while SMRs can extend this duration depending on the design and customer needs.

- Safety:

Microreactors can utilize passive safety features more effectively due to their higher surface-to-volume ratio and lower residual heat generation. Many designs rely on inherent physical properties and natural circulation for cooling, reducing the need for active safety systems. Traditional large reactors and SMRs can also be designed with passive safety systems but with greater complexity.

- Applications:

Microreactors are well-suited to remote and off-grid applications, such as remote research facilities, military installations, disaster response scenarios, or isolated communities. They can also serve as a reliable power source for industries in remote locations, e.g., mining sites. In contrast, traditional gigawatt-scale reactors and SMRs are typically used for grid power generation or to provide heat and power to a large industrial customer site near the nuclear plant site.

Given these characteristics, it is possible to analyze and identify areas of cybersecurity policies and frameworks that overlap between MMRs, SMRs and large reactors and also identify areas that require development Some of these overlaps and areas of development include:

- The U.S. Nuclear Regulatory Commission (NRC), in conjunction with international bodies such as the International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC), is working on the formulation of new cybersecurity requirements that address advanced reactors. [7].
- It is significant to note the areas of overlap that exist between the current cybersecurity frameworks for gigawatt-scale nuclear reactors and the emerging requirements for micro modular reactors. Critical digital asset identification and protection forms one such area, as these are systems whose compromise could jeopardize nuclear security or safety. The NRC and IAEA provide extensive guidance on this subject [8, 9].
- Further overlap exists in the implementation of the defense-in-depth strategy for cybersecurity. This multi-layered approach, aimed at preventing or mitigating cyber attacks, is highlighted in both NRC's and IAEA's revised guides [8, 9].
- Moreover, conducting computer security exercises is a common practice in the cybersecurity frameworks of both entities. These exercises simulate cyber attacks to test computer security measures and response capabilities, with both NRC and IAEA offering expertise and training in this area [7, 9].

However, certain aspects are unique to micro modular reactors and may require additional attention in cybersecurity frameworks. These include:

- Adapting to new technologies used in micro modular reactors.

Advanced materials, digital instrumentation, artificial intelligence, and advanced computational platforms introduce new potential vulnerabilities or challenges that need to be considered both in design and regulation [5].

- Addressing the increased multidimensional nature of cyber attacks

Potential attacks may target not only computer-based systems but also physical protection and detection systems, communication networks & supply chains. With the increasing types of cyberthreats globally and the increased use of more digital systems and processes, MMRs will have a higher number of vectors of cyberattacks. Coupled with the proposed remote operational model for MMRs and the potential operation of multiple units in parallel which could potentially require even more human operators compared to traditional reactor systems, there is a need to ensure that adequate safeguards in place to reduce the risk of these multidimensional vectors of attack [7]. Anticipating and preventing these attacks with complex, cascading consequences is vital for nuclear security and safety.

Recognizing the unique technical and regulatory challenges posed by micro-reactors, the NRC is working diligently towards comprehensive licensing applications [5]. In parallel, the IAEA is providing

guidance and training to enhance states' abilities to develop effective computer and information security activities for nuclear facilities. Recent initiatives include the issuance of their first implementing guide on computer security for nuclear security [9, 10] and international conferences to discuss the evolving dynamics of computer security within the nuclear domain.

3. Proposed Framework

As discussed in the previous section, MMRs have several differences with respect to large and reactors and SMRs. Hence analyzing their cybersecurity vulnerabilities needs a ground up approach. To perform this study, the following 7-step framework is proposed and used in the analysis for this study and visualized in Figure 2.

1) Segmentation of the System

   Here we would detail the division of the entire system into various integrated subsystems such as the Microreactor segment and the Remote Monitoring Center (RMC) segment. Each segment's role, importance, and function would be defined and explained.

2) Network Zone Identification

   Within each segment, this part would identify and explain the network zones, highlighting which zone handles which processes and the separation of zones for enhanced security. An emphasis would be placed on the need for network separation as a cybersecurity measure.

3) Threat Identification

   This section would focus on identifying potential threats and vulnerabilities in each network zone. The threats could be general cybersecurity threats or specific ones related to the operation of Modular Microreactors.

4) Risk Profile Analysis

   Using the Risk Management Matrix (RMM), this section would analyze each identified threat in each zone, creating a risk profile for each. This should include likelihood, impact, and potential consequences of the threat materializing.

5) Risk Mitigation Solutions proposed

   Based on the RMM, this section would propose solutions to reduce the cybersecurity risk for each identified threat. It should also discuss the potential effectiveness and consequences of implementing each solution.

6) Post-Mitigation Risk Analysis

   Here we would analyze the new risk profile with the proposed solutions. This analysis would consider whether the solutions effectively decrease the risks and whether any new risks or issues may arise from implementing the solutions.

7) Cost Analysis

   This section would provide a cost estimate for implementing the proposed cybersecurity solutions, potentially broken down by segment, threat, or solution. It should consider both initial implementation costs and ongoing costs, and balance these against the potential costs of failing to implement the solutions.

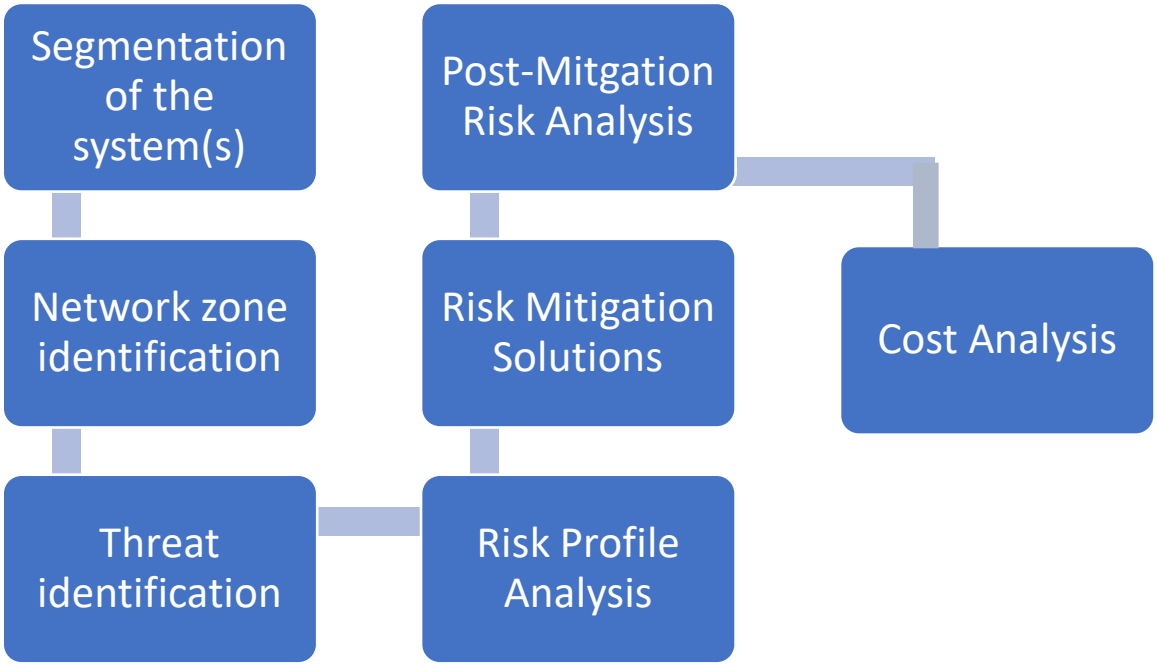

Figure 2 Proposed Cybersecurity Analysis Framework flow diagram

Each step would be represented by a box, with arrows leading from one step to the next. The flowchart could also include smaller boxes or notes underneath each step to provide more detail about what each step involves.

4. Identified threats

In the last section, we stated that for MMRs the main cybersecurity concerns would be those concerning an increased vector of attacks given their high utilization of digital computers and remote operations. Here we consider the type of threats both areas entail, beginning with remote operations.

When we consider remote operations, we have to look at the entire system in four different segments[1] (footnote to define segment):

1) The MMR segment
2) Remote Monitoring Center segment
3) Video Surveillance segment
4) Internet segment

Within each segment, we can identify blocks which will represent the various systems that exist within that segment thereby allowing us to analyze the type of cybersecurity vulnerabilities and connections between each block. To align with cybersecurity terminology, we will identify each block as a security zone[2] which would help narrow down the type of threat(s) and required cybersecurity policy and/or solution. This is visualized below in Figure 3.

[1] Network segmentation is a network security technique that divides a network into smaller, distinct sub-networks that enable network teams to compartmentalize the sub-networks and deliver unique security controls and services to each sub-network.

[2] A network security zone is an administrative name for a collection of systems that require the same access control policy. IP addresses are used to map systems into security zones.

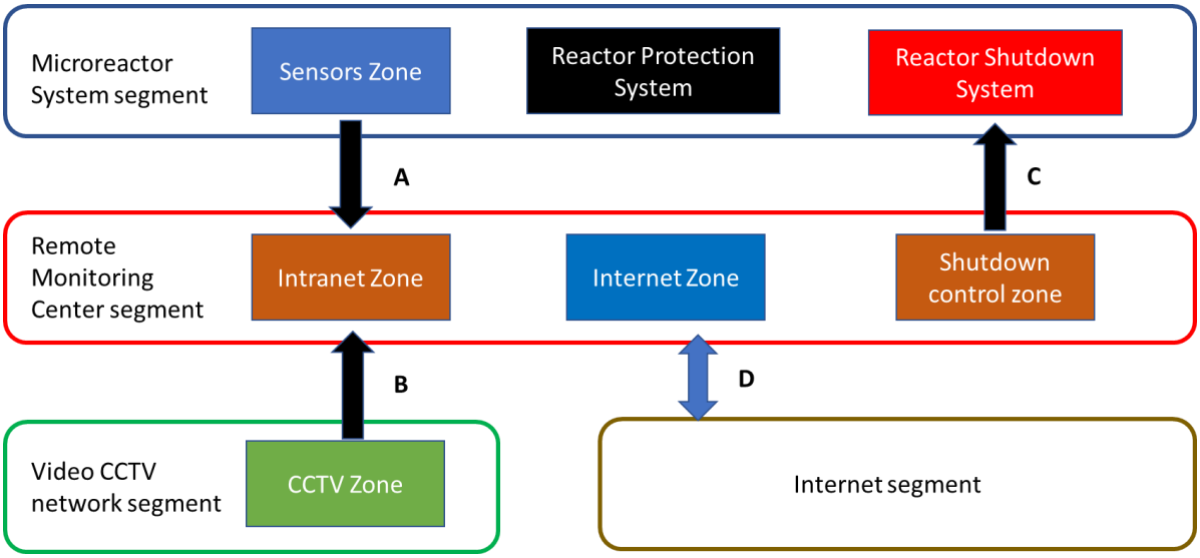

Figure 3 Recommended System & Network segment layout

4.1 Microreactor segment

The Microreactor segment represents all the physical systems within the MMR. By keeping the MMR segment on its own, we ensure that the analysis and framework are scalable to meet the needs for a potential fleet approach, i.e., multiple MMRs operating simultaneously. However, for the purpose of this study, we will assume a singular MMR for analysis.

In the absence of detail reactor designs, based on Figure 2 above, we have three main systems/zones within the MMR namely the Sensor zone, Reactor Protection System (RPS) and Reactor Shutdown System. The sensor zone will be where all the relevant sensors that monitor the reactor's parameters are placed. These sensors will ensure that the reactor operates within a defined set of parameters for the safe operation of the MMR. These sensors would transmit data back to the RMC and link directly to the RPS as the RPS is designed to force a SCRAM and activate the engineered safety systems in the event the sensors indicate the reactor is operating well beyond the set parameters.

Based on this context, we can summarize the communications to/from the sensor zone as follows:

Start zone	**End zone**	**Communication direction**	**One-way or bi-directional**
Sensor zone	RPS	Outgoing	One-way
Sensor zone	RMC – intranet zone	Outgoing	One-way

Table 1 Communication direction between sensor zone and end zone

From Table 1 above, by identifying the type of communications for the sensor zone, we can begin to identify the type of cybersecurity threats which could affect the sensor zone. Considering the main objective of the sensor zone is to ensure the operators and/or RPS are able to identify when the reactor is performing out of the acceptable parameter envelope, the main threat would be spoofing or modifying of the data that is coming out from the sensor zone. This could be done through several ways, namely:

1) Intercepting of signal when it leaves the sensor zone
2) Hidden backdoor programmed into the hardware prior to installation giving an external party remote command execution to modify the data autonomously (similar to a hidden FPGA backdoor threat)
3) Remote login/access of the sensors

Summarized below in the table are the identified threats for the sensor zone:

Threat identified	**Vector of attack**
Modification of sensor data before it reaches destination	Intercept outgoing signal to RMC segment
	Intercept outgoing signal to RPS
	Hidden backdoor in components that can receive a fixed command from external party
	Remote code execution or remote access of sensors from external network

Table 2 Summary of Threats to sensor zone

The next zone within the microreactor segment is the Reactor Protection System (RPS). As mentioned previously, the RPS is designated with only one objective and that is to SCRAM the reactor and activate the engineered safety systems in the event of a serious abnormal occurrence. Hence by design, the RPS is meant to operate completely autonomously and in a 'black box' fashion without the need for external intervention. However, the incoming communication from the sensor zone creates a single point of failure/threat. Hence the potential threats would be summarized as follows:

Threat identified	**Vector of attack**
Modification of sensor data before it reaches RPS	Intercept outgoing signal to RPS
	Hidden backdoor in components that can receive a fixed command from external party
	Remote code execution or remote access of sensors from external network
Remote code execution preventing RPS from performing function	Hidden backdoor in components that can receive a fixed command from external party
	Remote code execution or remote access of sensors from external network
Denial-of-Service preventing MMR from producing energy or preventing operator from accessing functions within the MMR	Remote code execution or remote access of sensors from external network

Table 3 Summary of Threats in the RPS zone

The final zone within the microreactor segment that has been identified through this work is the Reactor Shutdown System (RSS). The objective of the RSS is for the operator to initiate a *controlled* shutdown of the reactor (not a scram) typically for maintenance and or unplanned non-emergency shutdowns. Hence based on Figure 2, the RSS would only consist of one incoming communication from a system within the RMC segment's intranet zone and would not require any automation or sensor zone inputs. This would imply the potential threats to the RSS would be:

Threat identified	**Vector of attack**

Remote code execution preventing RSS from performing function	Hidden backdoor in components that can receive a fixed command from external party
	Remote code execution or remote access of sensors from external network

Table 4 Summary of threats in RSS zone

4.2 Remote Monitoring Center segment

The RMC segment as the name suggests, represents the systems and zones that are relevant to the operations of an MMR either in standalone remote location, a fleet of standalone operations or part of a grid-connected fleet configuration. Unlike traditional reactors or even SMR facilities like NuScale's which houses a RMC that manages the safety system controls for the reactor vessel and reactor cores, MMRs would house all safety related controls and systems within the MMR segment. Hence for MMRs, a RMC that would receive the incoming sensor data and allow operators to monitor the MMRs would be used in place.

For this paper, we will consider the case of a microgrid-connected fleet as that would represent a fleet of MMRs with multiple connections to a remote monitoring facility in its own isolated microgrid as seen in the figure below. Further considerations for connection of this isolated microgrid to the larger public grids, multiple remote monitoring facilities or renewable sources connected in the microgrid can be followed up in a further study.

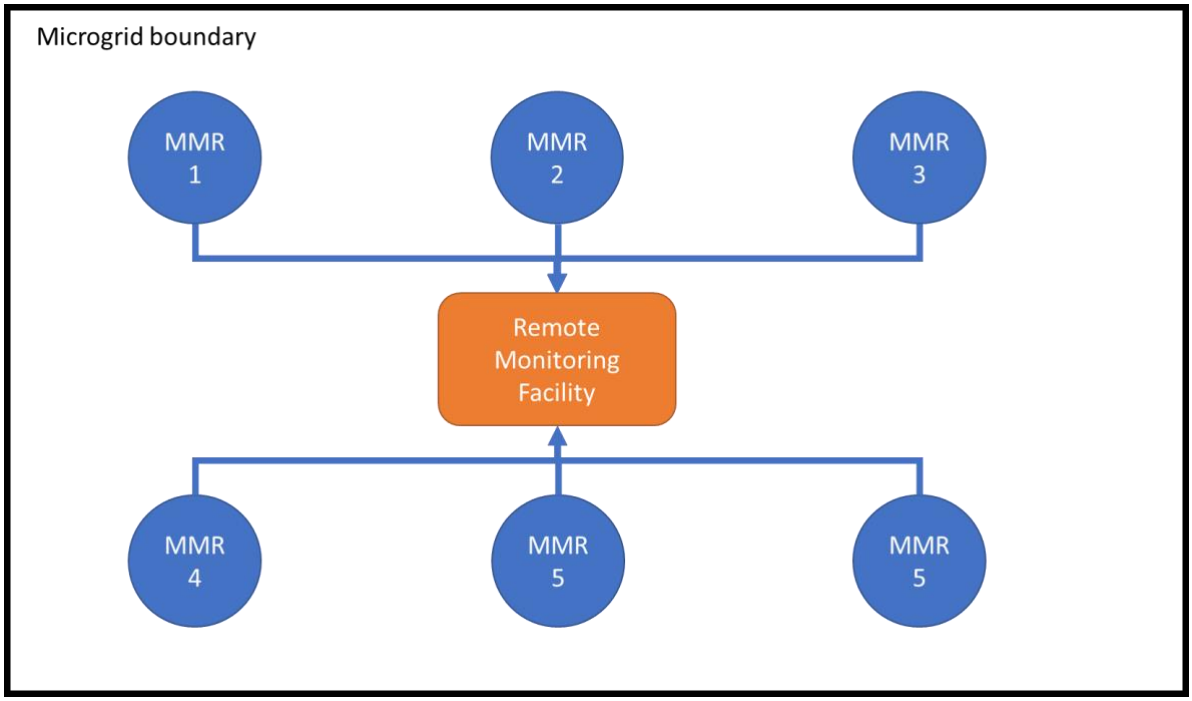

Figure 4 Microgrid MMR connection to a single remote monitoring facility

Within the RMC will sit the relevant systems and zones that facilitate the various types of communications required. As seen from Figure 3, this study has identified three basic zones:

1) The intranet zone: where the various mission-critical and MMR operational systems reside;
2) The internet zone: to facilitate communications with facilities and personnel outside the MMR and RMC intranet network; and
3) The controlled shutdown zone: Where the controlled shutdown system resides separately from the other zones.

The suggested architecture is meant to ensure that potential vectors of attack are minimized or eliminated altogether. More details about the use of network/zone separation will be covered in the section about potential solutions.

For the intranet zone, the following potential threats have been identified:

Threat identified	**Vector of attack**
Unauthorized access to mission systems	Physical unauthorized access to RMC and computers
	Unauthorized access to intranet network from external network
Remote code execution to interfere with intranet system	Hidden backdoor in components that can allow an unauthorized person from executing command through network connection
	Hidden backdoor in components that can allow an unauthorized person from executing command through physical access
Sensor network information modification	Physical unauthorized access to RMC and computers
	Unauthorized access to intranet network from external network

Table 5 Summary of threats in the intranet zone

For the Internet zone which houses the systems that require internet connection to communicate with systems and networks outside the RMC and MMR. Hence this zone is exposed to a wide variety of cybersecurity threats key threats summarized below:

Threat identified	**Vector of attack**
Malware	Internet Email system
Phishing	Worldwide web document download
Remote code execution and interception of email network	

Table 6 Summary of Threats for Internet zone

4.3 Video CCTV Surveillance

The final segment to analyse would be the CCTV video surveillance segment. This network represents the network of security cameras and surveillance devices that feed physical security monitoring information to the RMC to ensure the facilities housing the MMRs and the RMC are not breached by unauthorized personnel.

The summary of cybersecurity threats which could affect the Video CCTV Surveillance network is as seen in Table 7.

Threat identified	**Vector of attack**
	Intercept outgoing signal to RMC segment

Modification of surveillance data before it reaches RMC	Hidden backdoor in components that can receive a fixed command from external party
	Remote code execution or remote access of sensors from external network
Cutting of signal by severance of cable	Unauthorized access to cables/cable junction

Table 7 Summary of threats for the CCTV Surveillance zone and segment

In this section of the report, we have identified various potential threats that could be of concern for each segment and zone. The template in Appendix 1 can help to identify threats in a systematic manner. Many of the threats identified here align with those highlighted in the study performed by the Idaho National Lab (INL) [11].

However, it is impractical to design an entire cybersecurity system to remove the risk of all the threats. Hence, we need to understand what are the most important threats and develop cybersecurity solutions for those threats, while also minimizing the costs that will be added to the MMR's design.

5. Threat and risk level assessment.

The most common approach to rank the risk and threat level is to use a Risk Management Matrix (RMM). An RMM is a 2D matrix that combines the Likelihood level and Impact on the system, should that risk materialize. Impact here is defined broadly from disruption of service (with no nuclear safety consequences) all the way up to a severely abnormal occurrence that could lead to fuel degradation and possibly a radiological release. The levels of impact are defined below as follows:

- Negligible: There is no discernible disruption or impact to the operations of the MMR or the specific affected system and there is neither an effect on the of safety systems in operation nor a breach of sensitive information
- Minor: The affected system experienced a disruption which affected that specific system operation but it is isolated and did not affect any safety systems or operations of the MMR as a whole and there was no loss or breach of sensitive information
- Moderate: The affected system experienced a disruption which affected the operation of the MMR system as a whole but did not affect any safety systems and there was no loss or breach of sensitive information
- Severe: The affected system experienced a disruption which affected the operation of the MMR system as a whole with potential impacts on the safety systems and there was loss and/or breach of sensitive information
- Very Severe: The affected system experienced a disruption which affected the operation of the MMR system as a whole with an immediate and definite impact on the safety systems which leads to the safeties being unable to perform their functions and there was loss and/or breach of sensitive information

Both Likelihood and Impact are scored between 1 – 5 with 1 having the lowest likelihood and negligible impact and 5 being the highest likelihood and most severe impact. Then the product of the two numbers would allow us to assess how much of a risk would a specific threat carry. An example of the RMM is seen below:

It is important to stress that in an RMM exercise the scores are largely based on the analyst's judgment, so the scores shown in the following sections are meant to be representative and will have to be revisited by a panel of cybersecurity experts for each MMR design. The template in Appendix 2 can help perform this exercise in a systematic manner.

Risk = Likelihood x Impact		Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Highly Likely (5)
Impact	Very Severe (5)	Medium (5)	Medium-High (10)	High (15)	Very High (20)	Very High (25)
	Severe (4)	Low (4)	Medium (8)	Medium-High (12)	High (16)	Very High (20)
	Moderate (3)	Low (3)	Medium (6)	Medium (9)	Medium-High (12)	High (15)
	Minor (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium-High (10)
	Negligible (1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)

Figure 5 Risk Management Matrix

Through the RMM, we can identify threats which can be categorized into scores as follows:

a) Low risk profile: 1 – 4
b) Medium risk profile: 5 – 9
c) Medium-high risk profile: 10 – 14
d) High risk profile: 15 – 19
e) Very high-risk profile: 20 or greater

The main goal is to ensure that most threats are in the 'Low risk profile' category. Any threat that remains in the Medium-high to Very high range would need to be addressed and reduced by cybersecurity solutions.

Through the RMM, any current risk threat that lies within the 'Low risk profile' can be put on a low priority. With this, we can begin our analysis of the various threats identified in the previous section.

5.1 Microreactor segment

Analysing the sensor zone within the microreactor segment, we find the risk profile of the identified threats to be as follows:

Threat	**Likelihood Level**	**Impact level**	**Risk profile**
Modification of sensor data before it reaches final destination	Possible	Severe	Medium – high (12)

Table 8 Risk profile of sensor zone threat

Based on the type of threat and considering that from Table (8) there are three potential vectors of attack and given that the MMR would be some distance away from the RMC, the likelihood of intercepting and modifying the sensor data remotely or before it reaches the end zones is still possible due to the threat of implanting backdoors or potential intrusion points at the component level during manufacturing. In such an event, modification of the sensor data would result in a severe situation as it would impact the overall safety and operations of the system by having both the RPS and operators, who are required to monitor the incoming sensor data, to be operating under false data. Hence this results in a Medium – high risk profile for the sensor zone.

For the RPS zone within the Microreactor segment, we have three possible threats and their risk profiles as follows:

Threat	**Likelihood Level**	**Impact level**	**Risk profile**
Modification of sensor data before it reaches RPS	Possible	Severe	Medium – high (12)
Remote code execution preventing RPS from performing function	Unlikely	Very Severe	Medium – high (10)
Distributed Denial-of-Service (DDoS) preventing MMR from producing energy or preventing operator from accessing functions within the MMR	Rare	Moderate	Low (3)

Table 9 Risk Profile of RPS zone

In the case of the RPS zone, compared to the sensor zone, there are three types of threats each different from each other. For the case of the modification of the sensor data, with three possible vectors of attack as mentioned in Table 3 and the possibility of the components being compromised at the component manufacturing level, the likelihood would be 'Possible' with the effect being 'Severe' as it would impede the safety system of the MMR hence a Medium – High risk profile.

For the Remote code execution threat, unlike the modification of the sensor data threat, the likelihood of the threat occurring would be 'Unlikely' given that the remote code executions typically require an external command to be sent for activation. This would only occur if an active internet connection or insider personnel who has access to the communications panels exists. However, the impact from such a threat would be 'Very severe' given that a possible outcome would be a total shutdown of the RPS hence the overall risk profile is 'Medium – high'.

Finally, the DDoS threat is a very common type of cybersecurity threat faced worldwide by many industries. However, DDoS threats typically require connection to large number of networked computer and devices for a DDoS threat to be viable. Since one of the key design requirements is that most of the designed systems within an MMR would only have one communication pathway between zones, a DDoS attack, while possible, is highly impractical and would be a 'Rare' event with only a 'Moderate' impact as the RPS is designed to operate without any operator input hence a DDoS should not affect the outcome of the RPS and hence this threat would have a low risk profile.

The threats for the RSS would have the following risk profile:

Threat	Likelihood Level	Impact level	Risk profile
Remote code execution preventing RSS from performing function	Possible	Severe	Medium – high (12)

Table 10 Risk profile of RSS zone threats

For the RSS, the likelihood of a Remote Code Execution would be 'Possible' as there would be two vectors of attack and unlike the RPS which is designed to operate autonomously, the RSS can be accessed through control panels in the RMC. Hence should there be a built-in back door within the component level, it would be possible for unauthorised personnel to gain access through the RMC either by accessing the control system or an authorised personnel accidentally infecting the system through the use of an unauthorised USB drive which would shut down the RSS and create a 'Severe' impact. This results in an overall Medium – High risk profile.

In summary, in the Microreactor segment, we have considered five possible threats with four of them being Medium – high and one at the low risk profile. Therefore, on a first pass without any solutions considered yet, we would have four possible high-risk threats that would require addressing. These possible solutions will be covered in the next section of the report.

5.2 Remote Monitoring Center segment

Within the intranet zones the three threats highlighted have a risk profile as follows:

Threat	Likelihood Level	Impact level	Risk profile
Unauthorized access to mission systems	Unlikely	Severe	Medium (8)
Remote code execution to interfere with intranet system	Unlikely	Very Severe	Medium – high (10)
Sensor network information modification	Possible	Moderate	Medium (9)

Table 11 Risk profile of the intranet zone threats

In the case of the intranet zone within the RMC, we are assuming that intranet-based systems and networks would be practicing internet-separation and that access to the intranet network can be only performed on-site. As such, the occurrences of the threats of unauthorized access and remote code execution (which requires external commands to activate) would be unlikely as personnel who have access to the facilities on-site would traditionally have undergone background checks and be considered trustworthy. However, in the event should any unauthorized agent gain access to the facility or in the event of a rogue authorized personnel, they would be able to negatively affect the mission critical systems such as the sensor monitoring systems and resulting in a severe or very severe impact which creates a medium and medium – high risk profile respectively.

For the sensor network information modification threat, the likelihood would be similar to the Microreactor segment, but the impact lower as the RPS, which operates autonomously, would not be

affected by any false data readings by the operators in the RMC, i.e., the negative impact would be the RSS would not operate reliably.

For the internet zone within the RMC segment, the risk profiles of the three types of threats would be as follows:

Threat	**Likelihood Level**	**Impact level**	**Risk profile**
Malware *Phishing* *Remote code executions*	Likely	Negligible	Low (4)

Table 12 Risk profile of the internet zone threats

Unlike the other zones, we assume that all mission critical systems and zone would be separated from the internet hence while the likelihood of threats such as Malware, Phishing and Remote Code Executions is high given the rise of such incidences in recent years (insert ref), their impact to the overall operation would be negligible and hence all three would have a low risk profile.

5.3 Video CCTV Surveillance

For the final segment, the risk profiles of the threats identified are summarized below:

Threat	**Likelihood Level**	**Impact level**	**Risk profile**
Modification of surveillance data before it reaches RMC	Unlikely	Minor	Low (4)
Cutting of signal by severance of cable	Unknown	Minor	Low (4)

Table 13 Risk Profile of CCTV Surveillance threats

For the surveillance zone and segment, the identified risks would be low as it would not only require a high level of sophistication to modify the surveillance network and subsequently allow an unauthorised individual to access either the MMR, RMC or the cable junction boxes within the facility. Based on an effort-to-outcome ratio, it would be easier and faster for an unauthorised individual who has already penetrated the facility/compound to attempt access the intranet systems and/or sensor networks to modify the signals.

Finally, with regards to cable cutting (the so-called “tunnel threat”), while it is indeed a threat to the security of the MMR system, the physical access to the cables would fall under the purview of the physical security aspect hence beyond the scope of this study

In summary, in this section we looked at the various risk profiles of each identified threat to understand which threats carry a high risk. As part of the cybersecurity framework we propose, threats that are Medium – High risk or greater require solutions to reduce their risk level. In the next section we will go over some representative solutions which could be used to lower the cybersecurity risks for such threats.

6. Potential solutions to reduce cyber risks

This section of the report will focus on reducing the risk level of each high-risk threat to a low or manageable medium risk profile.

Each suggested solution would either lower the likelihood of the threat occurring, reduce the impact of the threat should the threat occur/breach has occurred or a combination of both. Given the short time frame for this project, we will consider only commonly adopted solutions. These solutions typically consist of the following:

Solution	**Intended function**	**Reduce likelihood/impact**
Data Diode	Ensures single-way communication preventing back communication	Reduces Likelihood
AES encryption	Encrypts the signal/data to prevent unauthorized personnel from reading and altering the data	Reduces impact
3-tier application architecture	Creates additional pathways for unauthorised individuals from accessing database tier and only allow access to the application through the app tier	Reduces likelihood
Secure certificates for authentication access	Ensures only authorised devices can access a system/network	Reduces likelihood
Role based account access	Ensures authorised personnel can only access certain systems/functions that are assigned to their role	Reduces likelihood and impact
Virtual private networks	Protects an entire network from breach if a sufficient level of encryption is used	Reduces likelihood and impact
Vendor/Supply chain management and validation	Ensures that components used by nuclear systems are validated and secured	Reduces likelihood and impact

Table 14 Common cybersecurity solutions

Based on the possible solutions above, we can suggest the following specific applications to each threat and their estimated reduction in risk profile:

Threat	**Solution**	**Old risk profile**	**New Risk profile**
Modification of sensor data before it reaches final destination	AES Encryption Data Diodes 3 tiered application architecture	Medium – high (12)	Medium (6)
Modification of sensor data before it reaches RPS	AES Encryption Data Diodes 3 tiered application architecture	Medium – high (12)	Medium (6)

Remote code execution preventing RPS from performing function	Vendor/Supply chain management and validation	Medium – high (10)	Medium (8)
Remote code execution preventing RSS from performing function	Vendor/Supply chain management and validation	Medium – high (12)	Medium (8)
Unauthorized access to mission systems	3 tiered application architecture Role based account access Secure certificates for authentication access	Medium (8)	Low (4)
Remote code execution to interfere with intranet system	Vendor/Supply chain management and validation	Medium – high (10)	Low (4)

Table 15 Summary of new risk profiles with solutions

From Table 15 above, using the suggested solutions would reduce the overall cybersecurity risk profile to acceptable levels. We also need to understand the estimated costs that accompany these solutions. One major challenge for this study is that certain solutions such as vendor management and establishing role-based account access are not fixed cost and would vary depending on the complexity of the system design. Hence for this paper, we would only consider the costs associated with fixed items based on our experience. Prices for items such as the data diode were set during 2021 and hence prices shown here are subject to change over time. (Change statement to say that the prices are subject to change over time as these values were obtained 2 years ago).

The fixed costs for Data diodes, AES encryption and 3-tiered application architecture are summarized and estimated in the table below:

	CAPEX
Data Diode	$90,000 SGD ≈ $68,000 USD (1SGD = 0.75USD) Per diode (inclusive of manpower costs)
AES encryption	Assume 6 months of software development and 1 software engineer ≈USD77,000[2]
3 – tiered software architecture	Assume 6 months of software development and 1 software engineer ≈USD77,000[3]

Table 16 CAPEX Table

This table above could be used to estimate the fixed costs for some of the solutions that need to be implemented. Note that while certain costs (e.g., data diodes) are present for each MMR, other costs (e.g., software development) are incurred only once for a fleet of MMRs.

7. Future work

The timeframe for this project was 3 months which limited the amount of analysis which could be performed. A study by the Idaho National Laboratory, the University of Massachusetts Lowell and the University of Tennessee Knoxville (insert ref) published in November 2021 highlights several other areas of work including new types of cybersecurity threats posed by AI and other solutions such as the use of digital twins to simulate attacks on the system and design suitable custom defences, Machine Learning techniques to pre-empt cyberattacks and complement operators when an attack is about to occur.

In addition, there is further work to combine the definitions of the severity of cybersecurity attacks on MMRs by considering both the effects of the attack on the systems, the outcome of the attack on the system and the relation to any potential radiological release.

These areas of follow-up would be pertinent to setting up a comprehensive cybersecurity framework which could aid in the licensing of MMRs at the factory manufacturing level.

8. Conclusion

This study has looked at a cybersecurity framework that could be applied to the analysis of MMRs as their development continues. This framework consists of breaking down a system into various segments and zones depending on the necessary security policy required and identifying the potential threats that could affect each zone. Identified threats for each zone are ranked according to likelihood and impact and their risk is assessed in a Risk Management Matrix (RMM). This approach allows a designer to determine which threats require immediate rectification at the design phase and which threats have a lower priority.

While this study was unable to investigate specific cybersecurity solutions in great technical detail due to the current early stage of MMR design, the framework proposed here could enable a much more efficient licensing process of these MMRs by addressing and resolving cybersecurity issues in the design stage.

References

[1] NuScale, “NuScale Power Unveils Name of Flagship SMR Plants as the Company Approaches Commercialization,” NuScale LLC, 02 December 2021. [Online]. Available: https://www.nuscalepower.com/en/news/press-releases/2021/nuscale-power-unveils-name-of-flagship-smr-plants-as-the-company-approaches-commercialization.

[2] Georgia Power, 2023. [Online]. Available: https://www.georgiapower.com/company/plant-vogtle.html.

[3] US Department of Energy, “DOE Microreactor Program,” [Online]. Available: https://gain.inl.gov/SitePages/MicroreactorProgram.aspx.

[4] C. Chenoweth, J. Green, T. Shaw, M. Shinn and G. Simonds, “The U.S. Nuclear Regulatory Commission's Cyber Security Regulatory Framework for Nuclear Power Reactors (NUREG/CR-7141),” USA Nuclear Regulatory Commission , November 2014. [Online]. Available: https://www.nrc.gov/docs/ML1432/ML14323A203.pdf.

[5] IAEA, “Computer and information security,” [Online]. Available: https://www.iaea.org/topics/computer-and-information-security.

[6] NRC, “US NRC Cybersecurity,” [Online]. Available: https://www.nrc.gov/security/cybersecurity.html.

[7] I. Garcia, “USA Regulatory Efforts for Cuberseecurity of Advanced Reactors,” March 2023. [Online]. Available: https://www.nrc.gov/docs/ML2304/ML23044A080.pdf.

[8] P. Samanta, D. Diamond and J. O'Hara, “Regulatory Review of Micro-Reactor - Initial Considerations,” 5 Feburary 2020. [Online]. Available: https://www.nrc.gov/docs/ML2004/ML20044E249.pdf.

[9] E. Lamce and S. H. Bolt, “IAEA Guidance on Computer Security for Nuclear Security,” 21 Oct 2021. [Online]. Available: https://www.iaea.org/newscenter/news/now-available-iaea-guidance-on-computer-security-for-nuclear-security.

[10] IAEA Computer Security Conference, “International Conference on Computer Security in the Nuclear World: Security for Safety,” [Online]. Available: https://www.iaea.org/events/cybercon23.

[11] C. Spirito, P. Lamb, S. Aghara, C. Duffley, J. Strandburg, J. Coble and F. Zhang, “Cyber Threat Assessment Methodology for Autonomous and Remote Operations for Advanced Reactors,” 2021.

Appendix 1: Threat identification template

Segment: _____ Zone: _____

S/N	Identified Threat	Risk Level*	Proposed solutions+	New risk level	Comment

* Use attached Risk Management Matrix for risk level identification. Use terminology from RMM

+ List out all proposed solutions in a list within the table

Appendix 2: Risk Management Matrix template

Segment: _____ Zone: _____

Threat: _____ Likelihood: _____ Impact: _____

Explanation for likelihood and impact choice:

Likelihood of Risk Occurring		Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Highly Likely (5)
Impact	Very Severe (5)	Medium (5)	Medium-High (10)	High (15)	Very High (20)	Very High (25)
	Severe (4)	Low (4)	Medium (8)	Medium-High (12)	High (16)	Very High (20)
	Moderate (3)	Low (3)	Medium (6)	Medium (9)	Medium-High (12)	High (15)
	Minor (2)	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium-High (10)
	Negligible (1)	Low (1)	Low (2)	Low (3)	Low (4)	Medium (5)