Cybersecurity in advanced reactor fleet by cyber-informed design, real-time anomaly detection, dynamic monitoring, and cost-effective mitigation strategies

Dr. Kaibo Liu (PI)

Department of Industrial and Systems Engineering

University of Wisconsin-Madison

Outline

- Introduction
- Research Challenges and Questions
- Proposed Research Tasks
- Summary

Introduction

- Microreactors are considered one of the most emergent areas in nuclear energy with disruptive potential.
  - In the future, there are proposed to be hundreds or thousands of microreactors simultaneously running as a fleet, with only 1 or even 0 staff needed on site.
- They will likely involve the use of semi-autonomous or highly automated industrial control systems (ICS).
  - These digital systems and wireless devices create unprecedented cybersecurity challenges to the nuclear industry.
- Existing regulations for commercial nuclear plants are not sophisticated enough to protect the future microreactor fleet from cyberattacks.
- This project will establish a series of advanced technical solutions tailored to future microreactor fleets, ranging from cyber-informed design (C-ID), real-time anomaly detection, dynamic monitoring, and cost-effective mitigation strategies.

Research Challenges

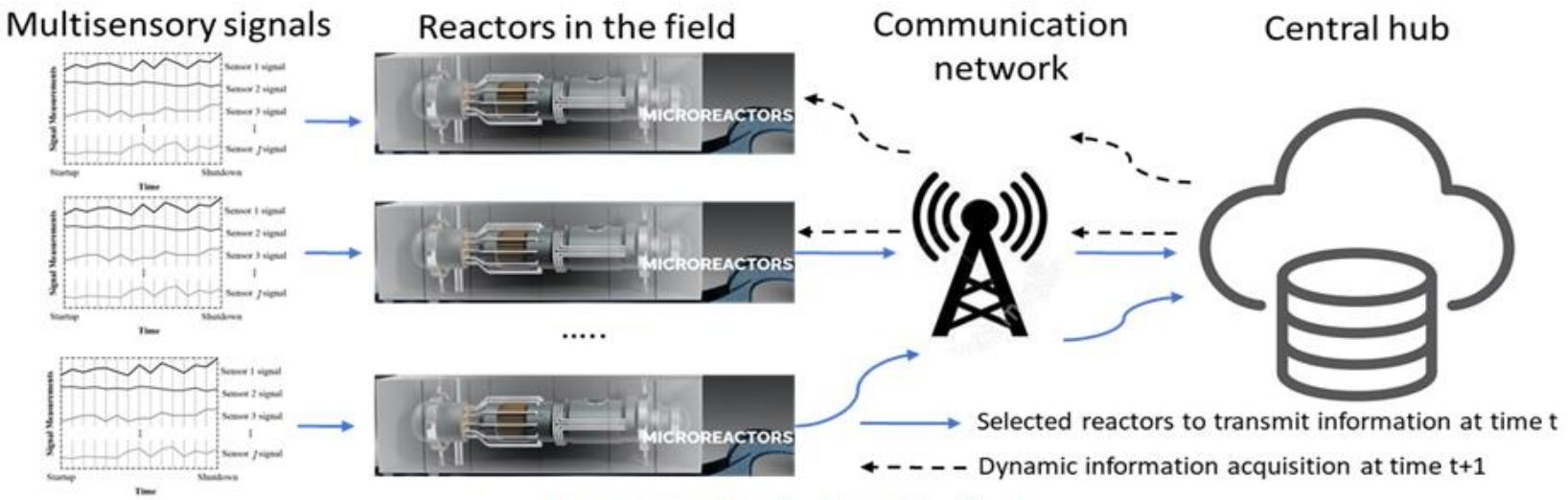


Fig. 1 Future microreactor fleet.

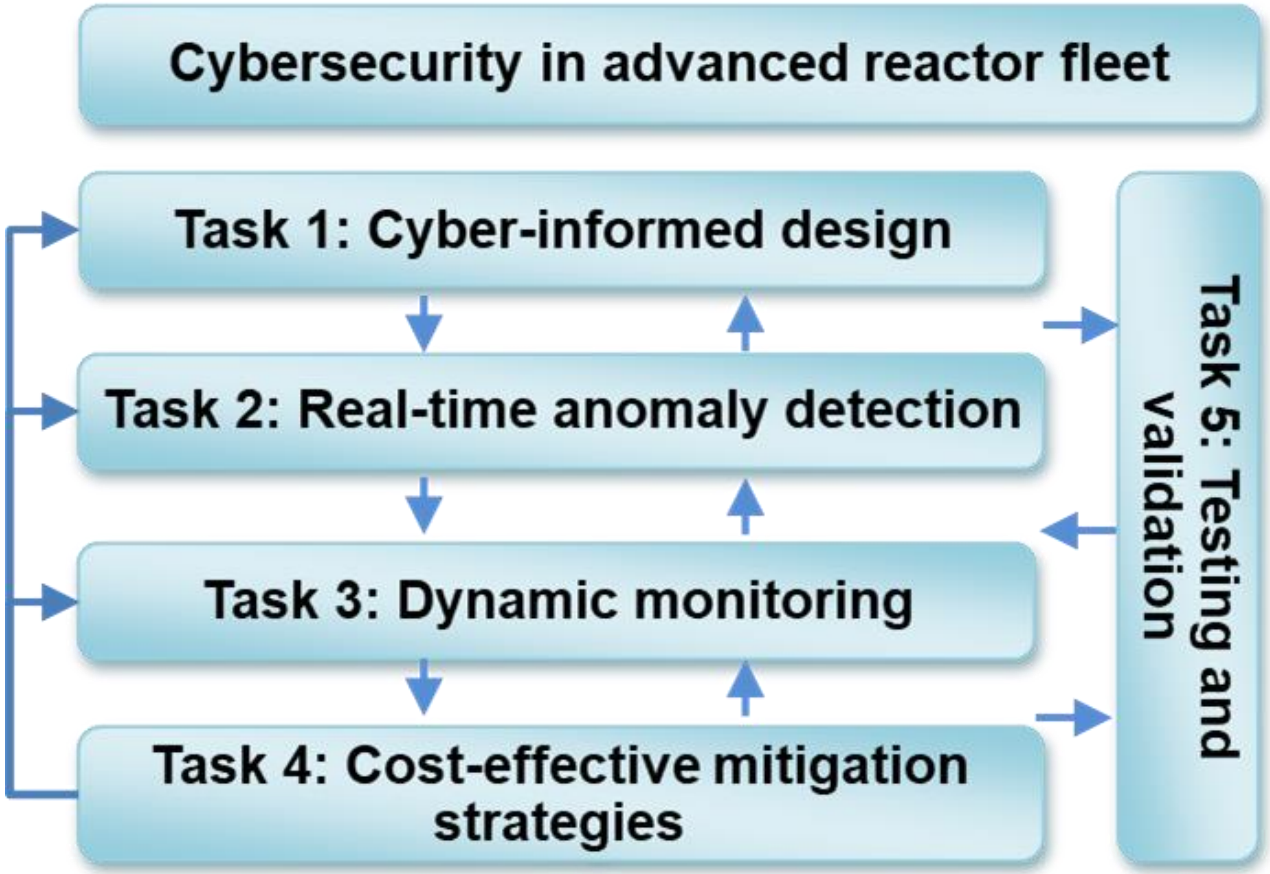
- The future microreactor: Collect multiple heterogeneous sensor signals for health surveillance in real time.
- The ICS of each reactor: Perform control and supervisory functions.
- The central hub:
  - Conduct remote monitoring by dynamically querying protected information from selected reactors given the bandwidth constraints.
  - Decide the optimal mitigation strategy for human intervention to identified microreactors when they are needed.

Research Questions

- There are significant challenges:
  - Cyber-informed Design (C-ID):
    - how to identify cybersecurity risks that exist in the integrated, coupled system
    - how to effectively conduct and continuously update C-ID
  - Real-time anomaly detection:
    - how to monitor heterogeneous sensor signals with different data distributions, physical meanings, noise levels, and sampling frequencies
    - how to detect new cyberattacks that continue occurring
  - Dynamic monitoring:
    - what information to transmit, when and which reactors to transmit information, and how the central hub leverages the received partial information to effectively monitor and manage the whole fleet
  - Cost-effective mitigation strategies:
    - how to prioritize the available resources to plan the most cost-effective mitigation strategies in a large fleet network

Proposed Research Tasks

- **Five inter-related research tasks will be developed:**



Task 1: Cyber-informed design

- Propose a mathematical modeling approach based on layered networks that evaluates risk.
- Explore the use of integer programming to identify a cost-effective set of mitigations to include to prioritize design decisions.
- When new risks/threats are identified, we will investigate what technical aspect of the microreactor network is affected, how and why the attack surface of the system is changed, which is helpful to continuously update the C-ID.

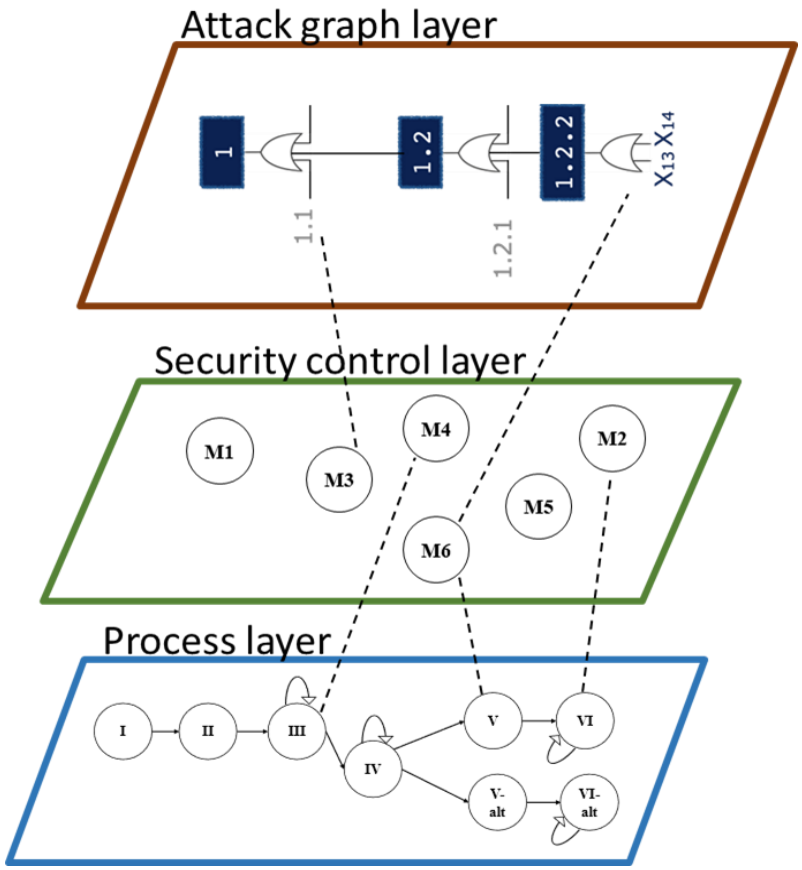


Fig. Layered networks for C-ID.

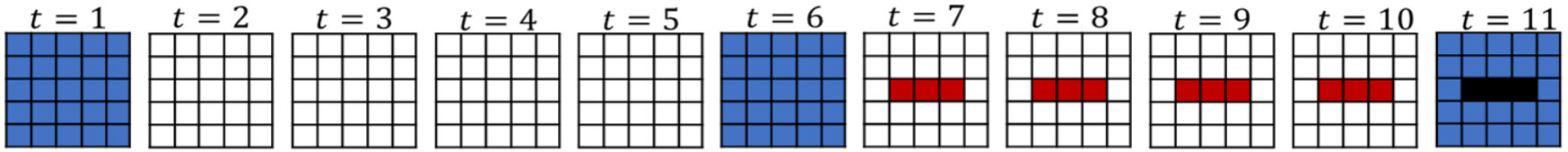
Task 2: Real-time anomaly detection

- We propose to closely monitor the residuals $X_j(t)$ between real-time observations and expected values of sensor j
  - $X_j(t)$ are heterogeneous with respect to j due to differences in data distributions, physical meanings of measurements, signal to noise ratios, and even sampling frequencies
- We plan to first establish an effective nonparametric online monitoring scheme that does not impose any distribution assumption on data streams and only requires training from normal operation data
  - Our novel idea is to monitor each data stream locally via a computationally simple and efficient nonparametric approach, and then combine all local schemes from different data streams together to produce a single monitoring statistic characterizing the status of each microreactor

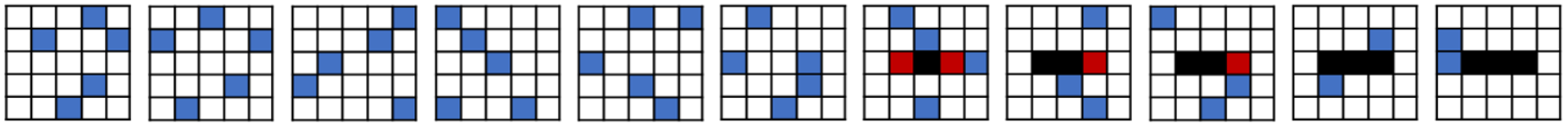
Task 3: Dynamic monitoring

blue: monitored microreactors **red:** anomalous microreactors

black: monitored microreactors overlapped with the anomalous ones



(i) Conventional monitoring strategy over the temporal domain (fixed monitoring interval)



(ii) Dynamic monitoring strategy over the spatial domain

Fig. Comparison between (i) the conventional monitoring strategy over the temporal domain and (ii) the dynamic sampling strategy over the spatial domain, where the total monitored microreactors by two schemes are the same.

- We will focus on the following technical questions:
  - what information to transmit
  - when and which reactors to transmit information back to the central hub
  - how the central hub leverages the received partial information to effectively monitor and manage the reactors at the fleet level

Task 4: Cost-effective mitigation strategies

- A central challenge is how to leverage the limited resources to optimally manage risk and intervene with minimal impact to degradation of microreactor performance.
- What are the worst-case risks and how can worst-case performance be bounded?
  - Built upon Task 3, identify which pathways require mitigation as well as the timeframe for the system identifying microreactors as anomalous by changing the transmit of the monitoring statistics.
- How and when to employ mitigation strategies in real time?
  - Leverage the Markov decision processes to decide the timing of various mitigating strategies using the output from Task 3

Task 5: Testing and validation

- The PIs will conduct synthetic simulation and real case studies to thoroughly test and validate the proposed methods.
- Synthetic simulation:
  - Dr. Zhang (Co-PI) hosts a state-of-art nuclear hardware-in-the-loop (HIL) cybersecurity testbed with a full-scope high-fidelity generic Pressurizer Water Reactor (GPWR) simulator and an Allen-Bradley Programmable Logic Controller (PLC).
  - Dr. Liu (PI)'s lab has a cybersecurity testbed using a set of interconnected Raspberry Pis to monitor the performance of battery (Pisugar2 Plus).
- Publicly available datasets: the cybersecurity challenges for ICS have existed for years in different industries
  - We will make efforts to collect existing data in the literature and several relevant use cases on the internet have been identified.
- IAB members:
  - Two leading companies in the nuclear field and one automotive supplier in automotive industry, are very excited to work with the research team for testing and validation and provide engineering time, expertise and data as needed.

Summary

- We intent to achieve the following outcomes:
  - scientific principles and integrated algorithms on cyber-informed design, real-time anomaly detection, dynamic monitoring, and cost-effective mitigation strategies for microreactor fleets;
  - programming codes implementing the algorithms;
  - simulation and real-world case studies and collected/generated datasets;
  - progress reports and final report summarizing findings and outcomes;
  - various conference presentations and journal publications
- The potential impact of the project will be significant and transformative
  - significantly enrich the existing literature by establishing new integrated suite of novel methodologies ranging from C-ID, real-time anomaly detection, dynamic monitoring, and cost-effective mitigation strategies
  - significantly improve the economics and effectiveness of cybersecurity risk management in future microreactor fleet

Schedule and Team members

Research Tasks	Year 1				Year 2				Year 3			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Task 1. Cyber-informed design (C-ID)												
Task 2. Real-time anomaly detection												
Task 3. Dynamic monitoring												
Task 4. Cost-effective mitigation strategies												
Task 5. Testing and validation												

- ***UW-Madison:*** Prof. Kaibo Liu (PI), Professor, Department of Industrial and Systems Engineering and Associate Director, IoT Systems Research Center. Prof. Laura Albert (Co-PI), David H. Gustafson Chair and Professor, Department of Industrial and Systems Engineering
- ***UM:*** Prof. Todd Allen (Co-PI), Chair, Department of Nuclear Engineering
- ***Georgia Tech:*** Prof. Fan Zhang (Co-PI), Assistant Professor, School of Mechanical Engineering
- ***Idaho National Laboratory (INL):*** Bri Rolston (Co-PI), Critical Infrastructure Security Researcher. Robert England (Co-PI), Instrument and Controls Research Engineer
- ***Industry Advisory Board (IAB):*** Westinghouse Electric Co. (led by Dr. Harold T. Maguire, Consulting Engineer for the eVinci Microreactor Program). Oklo Inc. (led by Dr. John Hanson, Senior Director). Lear Corporation (led by Dr. André Weimerskirch, Vice President for Cybersecurity and Functional Safety)

We greatly acknowledge the funding support by DE-NE0009404

Thank you!

Questions?