Federal Register Notice: 89 FR 78915, Federal Register :: Networking and Information Technology Research and Development Request for Information on Cyber-Physical Systems Resilience Research, September 26, 2024.

Request for Information on the National Cyber-Physical Systems Resilience Plan

Alina Zare, Ph.D.

Zoleikha Biron, Ph.D.

Swarup Bhunia, Ph.D.

Sara Rampazzi, Ph.D.

Sandip Ray, Ph.D.

UF | UNIVERSITY of FLORIDA

Herbert Wertheim College of Engineering
Associate Dean of Research and Facilities

[redacted]

Subject: Response to NSF RFI 2024-22005 - 'Cyber-Physical Systems Resilience R&D Plan'

Dear Suzanne H. Plimpton,

I am writing on behalf of the University of Florida, a leader in cyber-physical systems, resilience, and cybersecurity research, to submit our response to your recent Request for Information (RFI), NSF RFI 2024-22005 - 'Cyber-Physical Systems Resilience R&D Plan'. We are excited to have this opportunity to engage with the NSF community and share our expertise in addressing the pressing need for building Cyber-Physical System Resilience.

Our attached response to your RFI poses insightful suggestions, innovative ideas, and perspectives on resilience of critical infrastructure in the face of climate change, natural disasters or harsh environments (such as operating in the deep sea or in space). Our team has deep expertise in the relevant fields, with extensive experience in the research and development of cyber-physical systems and security of these systems. We also have research groups studying the resilience of our natural systems, coastal environments, and physical infrastructure in the face of climate change and several natural disasters (with a particular emphasis on hurricanes). We thoroughly understand the complexity of fortifying these systems while taking into account technical as well as social considerations.
In conclusion, we are excited to discuss our response further with you and look forward to future opportunities for research collaboration.

Sincerely,

[redacted]

Alina Zare, Ph.D.
Associate Dean of Research and Facilities, Herbert Wertheim College of Engineering
Professor, Electrical and Computer Engineering
Director, Machine Learning and Sensing Lab
University *of* Florida
a[redacted]

University of Florida's Response to NSF RFI 2024-22005 - 'Cyber-Physical Systems Resilience R&D Plan'

1. **Resiliency Challenges and Approaches in Critical Infrastructure Under Adverse Environmental Conditions due to Natural Disasters and Climate Change**
   Climate change is a stark and impending reality of our global environment. The very survival of critical cyber-physical system (CPS) infrastructure depends on our ability to be resilient against environmental impacts induced by climate change. It should be a research priority to determine (1) the impact of climate change on the functionality, safety, and sustainability of critical infrastructure and (2) strategies to make them resilient. Specifically, the transportation and energy sectors can be highly susceptible to the impacts of climate change in two ways. First, these infrastructures must achieve long-term sustainability in the transformed environment, e.g., a roadway or bridge must be resilient to higher temperature swings. Research in these areas marries the exploration of new materials (e.g., materials more resistant to extreme conditions) and research in AI and sensor technology (e.g., to identify aging or weakening infrastructure to enable effective and safe mitigation. Additionally, this research will heavily depend on exploring different resiliency strategies before deploying them in the infrastructure. One way to achieve this is through the practical design of digital twins for critical infrastructure that enables comprehension of their interaction with newer climate models.

   Many researchers at the University of Florida are at the frontier of observing and responding to natural disruptions, e.g., hurricane impact on built-, natural- and cyber-infrastructures. Much of this research area aims to encourage potential paths for novel and applicable technologies that enhance the resiliency of cyber-physical systems (CPSs) and significantly impact human life, society's revenue, well-being, and social welfare. The resiliency of CPSs toward natural disasters like hurricanes, wildfires, and earthquakes involves multiple strategies and technologies designed to withstand, adapt to, and recover from such events. Most existing research directions focus on preventing and minimizing the impacts of disasters. However, the stage of recovery and adaptable recovery of CPSs against abnormalities is as essential as restoring regular operation for CPSs. Such recovery strategies require localization of damages in widespread cyber-infrastructure, such as power systems, that may take days to finalize and stabilize.

   AI-based CPS resiliency during natural disasters, such as hurricanes needs to leverage advanced technologies to enhance preparedness, response, and recovery. However, most AI-based techniques require large training datasets. Yet, AI-based recovery and resiliency toward natural disasters suffer from limited datasets or facilities equipped with high-fidelity simulators that can simulate the event properly. Investigations to advance these techniques to develop a comprehensive research center that can simulate natural disasters for CPSs with exceptionally reliable models and develop adaptable AI-based resiliency approaches that learn from experiences are necessary. Such technology will not only enhance the resiliency of CPS but will also go beyond existing resiliency methods and make the recovered system wiser and more intelligent toward similar scenarios. Enhancing the resiliency of cyber-physical systems against hurricanes requires a multi-faceted approach that includes robust design, real-time monitoring, predictive analytics, and effective emergency planning. By integrating these

elements, organizations can improve their capacity to withstand natural disasters and recover more swiftly, minimizing disruption to critical services and infrastructure.

2. **Resiliency of CPS Systems in New Frontiers including, Deep Sea and Space**

The recently issued PCAST report, *Strategy for Cyber-Physical Resilience: Fortifying our Critical Infrastructure for a Digital World,* appropriately focuses on long-term improvements in critical infrastructure security, focusing on securing current national infrastructures such as Pipelines, Rail, Aviation, Water Systems, Ports, and Hospitals. All these areas merit research investment as these CPSs were not originally built with today's sophisticated AI-driven cyber-threats in mind, making them vulnerable to attacks that take advantage of intrinsic design vulnerabilities, legacy technology, and flaws in software and hardware domains beyond traditional network attacks.
AI-driven threats demonstrate adaptability even in the presence of incomplete or missing data, while defense systems are incredibly challenging to deploy and update on existing old infrastructures. We believe research priority should be given to attack-agnostic detection-reaction technologies and sematic-based approaches to analyze the behavior and relationships of data, AI models input-output relationships, and process flows to identify inconsistencies and determine the root cause of wrong automated and autonomous decisions.

The report does not, however, consider the security of emerging critical infrastructures deployed in isolated environments, such as deep sea and space. New underwater computing and storage platforms, commercial and military spacecraft, satellite swarms, and stations are a growing part of the global critical infrastructure, which deserves significant investigation.

Unlike traditional in-land infrastructures, such sparsely distributed, autonomous networks of moving and stationary systems are exposed to new threats that leverage the uniqueness of the environments in which they are deployed. University of Florida researchers have demonstrated that conventional security practices are insufficient to prevent data alteration or disruption of such CPS. We believe research is needed to revisit zero-trust architectures, enhance hardware and software side-channel resiliency, improve sensing and actuation technology robustness against novel physical and digital spoofing, advance autonomous security, ensure secure data storage and recovery, and maintain data integrity control over heterogeneous communication channels and across different physical mediums.
Research is also needed on innovations in tools and frameworks for rigorously testing software, hardware, and data security requirements during the design phase of such novel CPSs, which must withstand harsh environments and sophisticated attackers for prolonged periods without the possibility of immediate human intervention.

Summary of Response

Climate change poses significant risks to critical cyber-physical systems (CPS) infrastructure, especially in the transportation and energy sectors, necessitating research to enhance their resilience. The focus should be on understanding how climate change affects infrastructure functionality and developing innovative materials and AI technologies to improve safety and sustainability.

At the University of Florida, researchers are exploring strategies for CPS resilience against the increasing prevalence of natural disasters like hurricanes, emphasizing the importance of recovery processes alongside prevention. AI technologies are envisioned to enhance preparedness, response, and recovery, but require investment into systems that can generate simulated training data for training these AI technologies.

The PCAST report highlights the need for improved security in existing infrastructures, which were not designed for modern AI-driven cyber threats. It stresses the importance of developing attack-agnostic technologies to detect and analyze vulnerabilities. However, it overlooks the security of emerging critical infrastructures in isolated environments, such as deep sea and space, which are becoming increasingly significant. A comprehensive approach combining robust design, real-time monitoring, predictive analytics, and strategic emergency planning is essential to enhance CPS resilience against both natural disasters and cyber threats.

Key Findings and Recommendations

Key Findings:

1. **Climate Change Impact:** Critical infrastructure, particularly in transportation and energy, is highly vulnerable to the effects of climate change, necessitating research on functional sustainability.
2. **Resilience Strategies:** Existing research often focuses on disaster prevention, but effective recovery and adaptive strategies are equally important.
3. **AI Limitations:** Current AI-based approaches for enhancing CPS resilience face challenges due to limited training datasets and the need for high-fidelity simulators for disaster simulation.
4. **Cyber Threat Vulnerability:** Many existing CPS infrastructures were not designed to withstand modern AI-driven cyber threats, making them susceptible to attacks exploiting inherent vulnerabilities.
5. **Emerging Infrastructures:** Security considerations for new CPS in isolated environments like deep sea and space are currently underexplored.

Recommendations:

1. **Research Prioritization:** Invest in research to assess the impact of climate change on critical infrastructure and identify resilience strategies.
2. **Enhancing Recovery Strategies:** Develop comprehensive recovery plans that focus on rapid damage localization and adaptable recovery processes in CPS.
3. **Advanced AI Techniques**: Create improved AI models that can learn from past experiences and effectively simulate natural disasters, ensuring they are equipped with extensive training datasets.
4. **Attack-Agnostic Solutions:** Focus on developing detection-reaction technologies that analyze data relationships and identify inconsistencies, enhancing security against evolving cyber threats.
5. **Explore Isolated Environments:** Increase research attention on the security of critical infrastructures in isolated environments, including underwater and space systems, acknowledging their growing significance.

By addressing these points, organizations can enhance the resilience and security of critical CPS against both environmental and cyber threats.

Conclusion
We hope that our response has provided valuable information and insights that can inform future research directions and decisions at the NSF. We look forward to the opportunity to discuss our response further and explore potential research collaborations.

Sincerely,
Zoleikha Biron, Ph.D.
Swarup Bhunia, Ph.D.
Sara Rampazzi, Ph.D.
Sandip Ray, Ph.D.
Alina Zare, Ph.D.
University of Florida

Notes: Dr. Kevin Butler recused himself from this response because he is on the PCAST Review Working Group. This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in the National Cyber-Physical Systems Resilience R&D Strategic Plan and associated documents without attribution.