Teaching Philosophy

Training Resilient Minds for a Resilient AI+X Future

As extreme-scale AI systems become the driving force of modern research [1], *the next generation of scientists cannot merely use supercomputers; they must be experts in resilient engineering* [2]: capable of diagnosing complex hardware/software reliability failures and securing petascale research data against sophisticated threats [3]. Successful integration of my teaching agenda into your department will yield:

i) **Curricula on Resilient and Secure AI**: Developing an AI Failure Modes course depicting limitations of AI tools, while engineering a new graduate-level course on Resilient and Secure AI supercomputing.

ii) **Funding an Exotic Systems Lab**: Securing funding to establish an Exotic Systems Lab with emergent computing capabilities (e.g., connecting with exascale supercomputers, HPC-Quantum Computing integration, novel failures and security backdoors), supported by the over $1.8M in grants I have secured.

iii) **Steady Student Career Pipeline**: Providing a steady student career pipeline into critical roles at DOE, industry, and research computing institutions, demonstrated by my undergraduate students securing jobs at Sandia, Argonne, FAANG, etc., and publishing in top venues like IEEE Quantum Week.

iv) **National Influence in Cyberinfrastructure and Research Security Education**: Achieving national influence in Cyberinfrastructure and Research Security Education, through partnership with the NSF Cybersecurity Center of Excellence (Trusted CI Fellow) and curriculum validation efforts with NAIRR.

My proposed curriculum is *Resilient AI+X*, where *X* represents emerging supercomputing/HPC, GPU, and quantum architectures [4]. My teaching philosophy is to translate real-world disruptions of Leadership Class Computing Facilities (LCCF) into engaging forensic experiences for students, ultimately leading to deployable mathematical models that preempt accidental failures and intentional cyberattacks. This teaching approach is viable due to my unique background at the National Center for Supercomputing Applications, where I worked closely with other supercomputing centers (TACC, OSG), DOE national labs (SLAC, Argonne, ORNL, Berkeley Lab), and federal agencies (NSF, NIST).

Teaching Philosophy: Cultivating a Resilient Mindset

The core of my teaching philosophy is to cultivate a **resilient mindset**, one that views system failures and security breaches not as final endpoints, but as rare learning opportunities with a rich dataset. I emphasize the *Measurements* $\rightarrow$ *Modeling* $\rightarrow$ *Impact* paradigm, grounded by unique access to the data lake of real-world Leadership Class Computing Facilities (LCCF) and supercomputers, in my teaching.

1. **Measurements-Driven Education:** Students learn how to instrument, collect, and curate cross-stack data from interdisciplinary fields. They apply **probabilistic modeling** (e.g., Bayesian Networks, Factor Graphs) and then validate these models against real system behavior with expert knowledge. This hands-on experience provides a critical lens for building verifiable, reliable systems. I integrate this directly into coursework, such as a hypothetical "Probabilistic Graphical Models for Security" course, where students validate their security models against real system behavior.

2. **Connecting Real-World Systems with Learning:** I integrate my unique, petabyte-scale datasets—including performance logs from the **Blue Waters** supercomputer, GPU failure measurements, and forensic security traces—directly into coursework. Students analyze real-world incidents, such as GPU 'melting' under extreme load or sophisticated cyberattacks, to understand system vulnerabilities and error propagation across the hardware-software stack. This turns abstract concepts like "dependable systems" into tangible, high-stakes engineering challenges, focusing on evaluating the **quantifiable risk** of attack or probability of failure.

New Courses: Resilient AI+X (HPC, Networking, Quantum)

The convergence of AI, quantum computing, and high-performance computing (HPC) demands updated educational approaches that equip students with hands-on experience using novel hardware and accelerators. To meet this challenge, my primary teaching plan is to develop and implement a new curriculum under the theme of **"Resilient AI+X."**

Undergraduate and Graduate Course Proposals

Course Title	Level	Syllabus summary and Course outcome
AI Failure Modes 101	UG	Key concepts of generative AI (data source, hardware (GPU), software (training and inference)) with the focus on uncertainty in each step. This will illustrate how automating AI through agents can fail in different real-world conditions (healthcare, system diagnosis, etc.). I will leverage my national lab collaborations and AI pilot program, like NAIRR, to provide hands-on classroom resources.
Resilient AI+X: Systems & Architectures	Upper UG / Grad	I will modernize traditional reliability concepts (e.g., Mean Time To Repair [$MTTR$], Mean Time Between Recovery [$MTBR$]) for X, which can include HPC, Quantum, and emerging interconnects such as NVQLink or Qiskit/CUDA-Q simulators. The course integrates component- and system-wide reliability measurements into quantitative real-world AI workloads on GPUs from DOE and DeltaAI.
Dependable Systems and Networks (DSN) Modeling	Graduate	The course will adopt my 'Measurements $\rightarrow$ Modeling $\rightarrow$ Impact' paradigm. Students will utilize high-fidelity, petabyte-scale datasets to develop and validate both formal models and probabilistic graphical models that predict system failure or attack statistics, thereby making system dependability quantifiable and practically verifiable from design to deployment.

Demonstrated Teaching and Mentorship Success

My teaching and mentorship success is evidenced by the immediate career placement of diverse students (domestic and international) in critical national and industry roles. Mentees have secured key positions at DOE National Laboratories, including Neil Rayu at Sandia and Hung Nguyen at Argonne National Lab , while others joined major firms like Microsoft and KPMG consulting. Both mentor and students have been recognized with Fiddler Innovation awards, and published in a leading IEEE conference on Quantum Computing and Engineering [5]. The impact of my teaching has extended beyond the classroom, as demonstrated by NSF awards in research security education that have influenced national-scale policies on securing research computing.

Influencing National Policy on AI Education

My long-term goal is to establish a national standard for AI education that mandates integrating system resilience, cybersecurity, and real-world, data-driven problem-solving across all advanced AI/HPC/Quantum curricula. My teaching and curriculum development will directly feed into this goal by:

(1) **Phase 1: Curricular Validation** by using student performance and project outcomes in the "Resilient AI+X" course sequence as the evidence base. (2) **Phase 2: Policy Dissemination** by packaging the validated curriculum and delivering it to AI-leading policy and educational efforts (e.g., NIST, NAIRR).

Students[1] mentored by me have found success in critical positions at national labs (Sandia, Argonne) and FAANG companies, a benchmark of success I expect to continue with your student body.

My teaching plan will provide rigorous preparation for both students and industry, define the standards for national-scale AI supercomputing education, and attract both engineering and business students.

[1] Students' anonymized testimonies and teaching evaluations will be available upon request.

APPENDIX

HPCwire SECTORS

NCSA Awards 17 Students Fiddler Innovation Fellowships

Feb. 4, 2025 — The National Center for Supercomputing Applications awarded Fiddler Innovation Fellowships to 17 University of Illinois Urbana-Champaign and NCSA graduate students in a ceremony January 28 honoring the outstanding achievements and interdisciplinary contributions to NCSA programs Students Pushing Innovation (SPIN) and Design for America during the 2023-24 academic year.

The awards are part of a $2 million endowment from Jerry Fiddler and Melissa Alden to Illinois in support of student and faculty interdisciplinary research initiatives through the Illinois Emerging Digital Research and Education in Arts Media (eDream) Institute at NCSA.

Jakub Sowa, mentored by Phuong Cao, has been awarded with the fellowship by Professor William (Bill) Gropp.

https://www.hpcwire.com/off-the-wire/ncsa-awards-17-students-fiddler-innovation-fellowships/

Students and Mentors touring the National Petascale Computing Facility took time to pose in front of the newest NCSA supercomputer, Delta.


At NCSA, important research is being done every day. Everything from working towards better cancer treatments to studying supernovae is included in NCSA's portfolio of research projects. But NCSA doesn't stop there. The Center also wants to help train and inspire future researchers. Through our many undergraduate student research opportunities, NCSA offers hands-on time with ongoing research with experts in their fields. The NCSA-funded Students Pushing Innovation (SPIN) and the National Science Foundation (NSF) -funded Research Experiences for Undergraduate (REU) programs both provide a one-of-a-kind experience for students interested in careers in research. By embedding REU and SPIN students in the projects, the students learn how research is conducted while working toward a research goal.

Students presenting at the STEM Career Exploration and Symposium

Being embedded on research teams isn't the only opportunity available to SPIN and REU "The Future of Discovery: Training Students to Build and Apply Open-Source Machine Learning Models and Tools" (FoDoMMaT) students. NCSA interns and fellows are also encouraged to participate in professional development via conference attendance and participation. Students are supported by their mentors and the administrators of these programs, and funding for conference fees and materials is provided by NCSA. This year, students participated in the Grainger College of Engineering's annual Engineering Open House, with SPIN students winning first place for their exhibit. SPIN and REU FoDoMMaT students also participated in the STEM Career Exploration and Symposium. As members of the Illinois Summer Research Programs Alliance (ISRPA), the students represented NCSA's programs in a this summer's event. The symposium had 120 student presenters across ISRPA and over 400 attendees. During the symposium, students engaged with 13 different industry partners and six professional organizations. They also reached out to 53 community college students and educators from across the state and helped them see the possibilities within the STEM field.

https://ncsa.illinois.edu/2023/08/09/undergraduate-researchers-in-action/

Mentoring and Diversity Statement

Supercomputing for All is my approach to increasing participation in the area of AI for Science. My career as a Principal Investigator and Research Scientist at the intersection of supercomputing (HPC) and cybersecurity is defined not only by the pursuit of resilient, secure systems, but also by a commitment to building an inclusive environment, helping students to exceed their growth potential.

Mentorship and Students Development The student cohort that I have introduced to the power of supercomputing, and the importance of secure computing as well as data security, includes domestic undergraduate NSF CyberCorps Scholarship for Service (SFS) program and NCSA's Students Pushing Innovation (SPIN) students, international graduate students, and visiting postdocs through the European Next Generation Internet Enrichers and Vietnam Education Foundation's Fellowship. Having benefited from international education and mentorship advised by excellent professors as well as industry leaders, I pay it forward by mentoring a diverse group of domestic students, students from underrepresented and international backgrounds, equipping them with resources to fully realize their potential.

My goal as a mentor goes beyond technical skill transfer; it is focused on building core research skills (critiquing papers, scientific visualization, and giving research presentations) that are traditionally not taught in dedicated classes. This was recognized by the "Outstanding Mentors" award for a Fiddler Innovation Fellowship awardee. For instance, I guide undergraduate students through complex research like "Post-Quantum Cryptography (PQC) Network Instrument" and help them transition into leading roles at institutions like Microsoft Security Copilot, Argonne National Lab, and Sandia. In my research, I prioritize providing a pathway for individuals who traditionally lack access to the high-performance computing domain.

Making Supercomputing/HPC Accessible to All The highly specialized field of high-performance computing and complex security protocols can feel exclusionary to a small group of students. To address this, I have engaged in outreach designed to make the field more accessible. For example, I have given several tours of the National Petascale Computing Facility at Urbana, IL, to groups of both students and faculty, as well as teaching basic security concepts, e.g., authentication and authorization, to K-12 students at Carrie Busey Elementary School, giving them a head start and awareness of the importance of security concepts.

My teaching, including developing machine problems and guest lecturing in courses like "Trustworthy AI Systems" and "Dependable AI Systems," is designed to give students concrete real-world examples that are immediately useful for their interview preparations and real-world jobs. I am acutely aware of the different interpretations and knowledge of students from different backgrounds to ensure that advanced concepts are taught with an emphasis on clarity and ethical implications, making the material digestible to students from various academic and cultural backgrounds.

Research and Systems with Inclusive Impact To tie it together, my research agenda, which focuses on building resilient systems and combating cyber threats through AI-driven malware analysis and quantum-resistant cryptography, implicitly serves a diversity mission. Secure and reliable cyberinfrastructure, such as the petabytes of data curated on supercomputers like Blue Waters and Delta, is essential for open-science research. Ensuring supercomputers are dependable means that researchers from all institutions, including those with fewer resources, have equitable access to the computing power needed for scientific discovery. My projects, funded by grants from NSF and IBM, are explicitly designed with an education mission in mind to bring reliable and highly available computing resources accessible to a maximally diverse research community.

In sum, I have engaged a broad group of students to advance the motto Supercomputing for All. In the future, I will continue to bring the latest advances in AI-HPC-Quantum integration to inspire the next generation of students.

References Cited

[1] "Energy department announces new public-private partnership model, two supercomputers, to accelerate american dominance in science and technology | department of energy." https://www.energy.gov/articles/energy-department-announces-new-public-private-partnership-model-two-supercomputers, 10 2025. [Online; accessed 2025-11-07].

[2] S. Cui, A. Patke, H. Nguyen, A. Ranjan, Z. Chen, P. Cao, B. Bode, G. Bauer, C. Di Martino, S. Jha, *et al.*, "Story of two gpus: Characterizing the resilience of hopper h100 and ampere a100 gpus," *Supercomputing, ACM/IEEE International Conference for High Performance Computing, Networking, Storage, and Analysis*, 2025.

[3] P. M. Cao, Y. Wu, S. S. Banerjee, J. Azoff, A. Withers, Z. T. Kalbarczyk, and R. K. Iyer, "CAUDIT: Continuous auditing of SSH servers to mitigate brute-force attacks," in *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, pp. 667–682, 2019. https://www.usenix.org/conference/nsdi19/presentation/cao.

[4] B. Baheri, E. Giusto, S. Xu, K. N. Smith, E. Younis, and P. Cao, "Grand challenges of secure & trustworthy quantum computing," 2025.

[5] J. Sowa, B. Hoang, A. Yeluru, S. Qie, A. Nikolich, R. Iyer, and P. Cao, "Post-quantum cryptography (PQC) network instrument: Measuring PQC adoption rates and identifying migration pathways," in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, vol. 1, pp. 1835–1846, IEEE, 2024. https://doi.org/10.1109/QCE60285.2024.00213.