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 101 literacy course on critical thinking (in development with NAIRR), while developing a new graduate-level course on Resilient and Secure AI supercomputing.

ii) **Funding and Innovative Systems Lab**: Securing funding to establish an Innovative Systems Lab with exotic computing capabilities (e.g., exascale supercomputing, HPC-Quantum Computing integration, and resilient/secure AI), 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 students securing jobs at Sandia, Argonne, FAANG, etc., and publishing in venues like IEEE Quantum Computing and Engineering.

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 Literacy 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, influencing 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 the integration of system resilience, cybersecurity, and real-world, data-driven problem-solving into 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 policy-making bodies (e.g., NIST, NAIRR).

My proposed teaching plan will provide rigorous preparation for both students and the industry, defining the standards for national-scale AI supercomputing education.

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.

Appendix

Exhibit 1: Teaching Evaluation

Exhibit 2: Student Testimonies