



# Making AI Work for Science: Data, Models, Security, and Embodiment

May 14, 2026

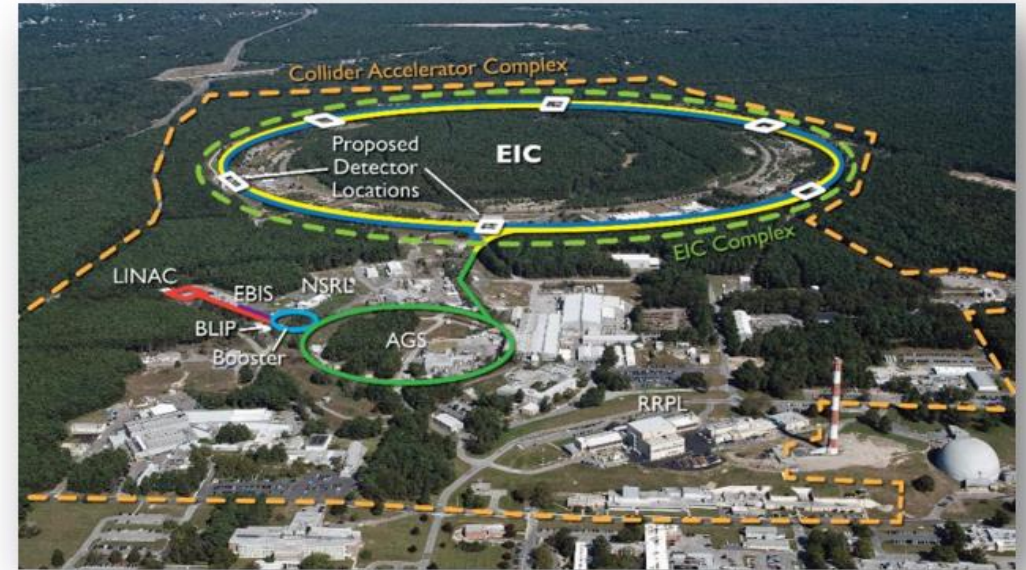
Carlos Soto  
AI Department

# AI for Science

## Improve scientific work

- Faster
- More efficient
- More productive
- More thorough
- Better performance
- Higher throughput

## Enable something new



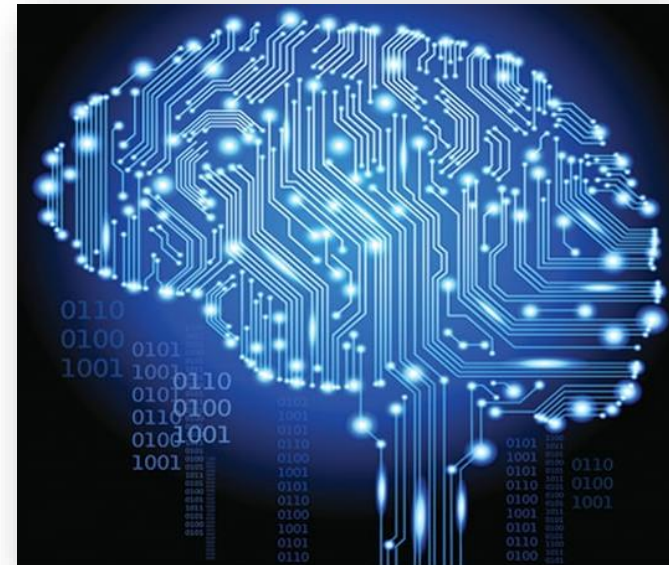
# AI for Science

Science is not a factory; it's a workshop, a lab

- Novelty is the point → accelerating techniques need to support **dynamism**

Many roles of AI in science already

- Perception
- Analysis & inference
- Ideation/hypothesis generation
- Simulation surrogates
- Design & control of experiments
- Inverse modeling
- Data management, filtering, compression
- ...



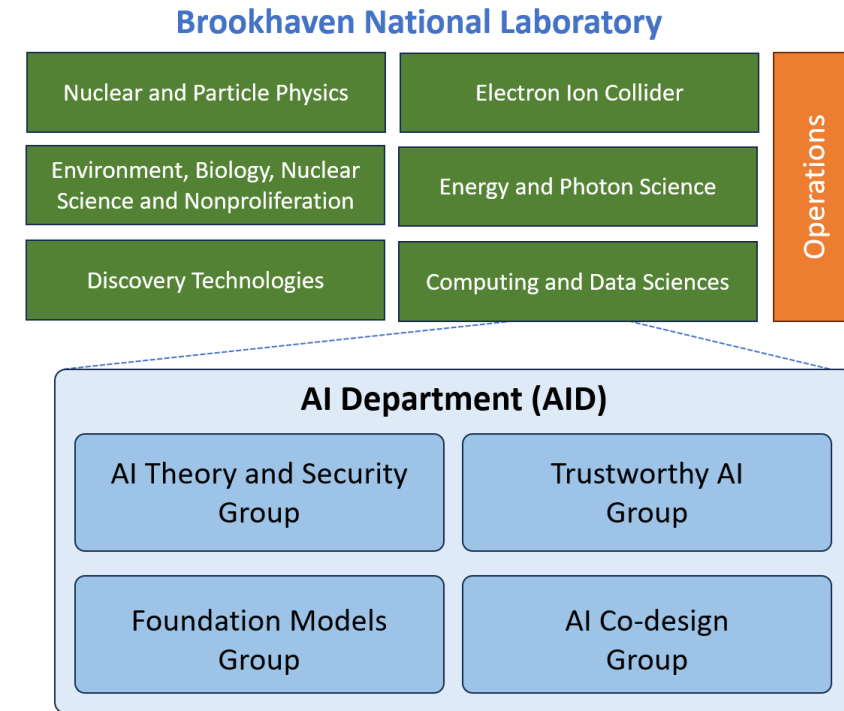
# AI research & impact at BNL

## AI Applications

- Collaborations with all scientific directorates at BNL

## AI Fundamentals

- Much less common among national labs



Quiz:

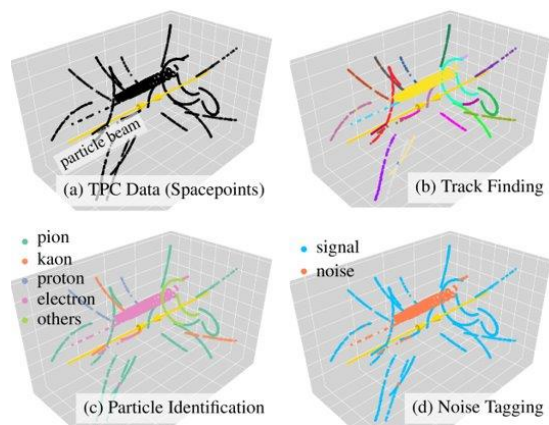
NeurIPS, ICLR, ICML, ACL, EMNLP, COLING, CVPR, ICCV, ECCV

AI as a **Science**, not just a technology

# Designing AI for Unique Data Needs

## Scientific Data

- Massive datasets
- Streaming analysis
- Heterogenous, multi-source
- Spatiotemporal, dynamic
- High sparsity



Particle collision tracks from RHIC (*above*), data transformations (*above right*), part of BNL's novel AI model design (*right*).

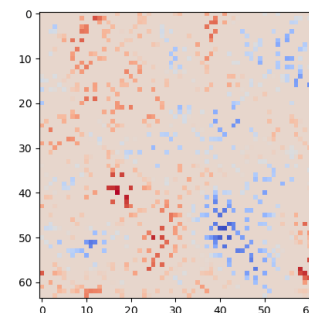
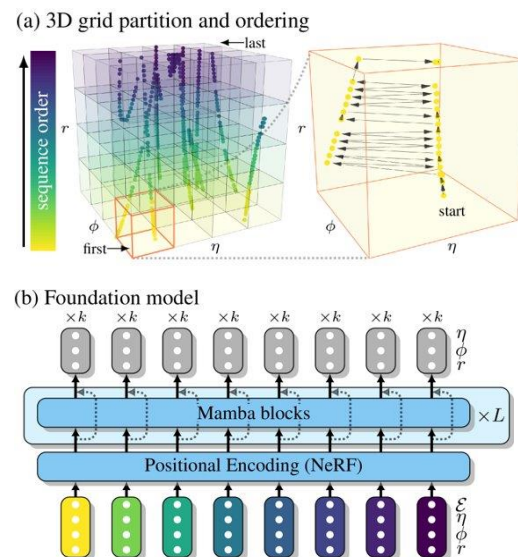
## Foundational developments, state of the art results

Novel algorithms and innovations in

- Foundation model design
- Training and optimization strategies
- Physics integration

Experimental results

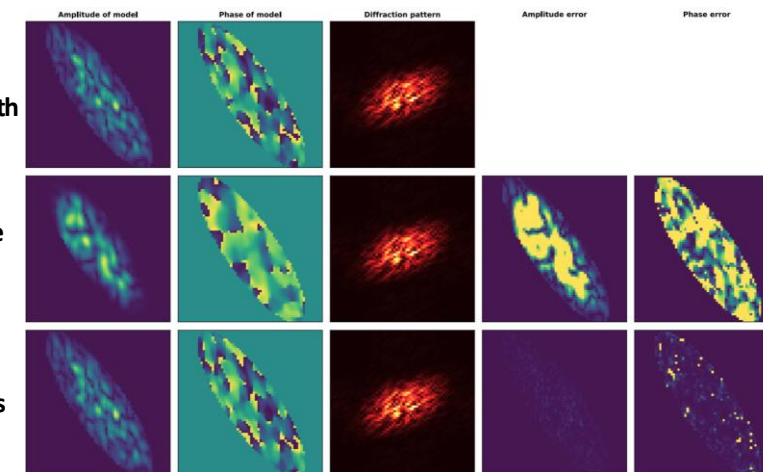
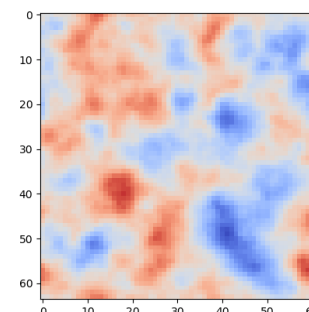
- Outperform competing methods
- Regularly publish in top AI conferences (NeurIPS, ICML, ICLR, AAAI, etc.)



Ground truth

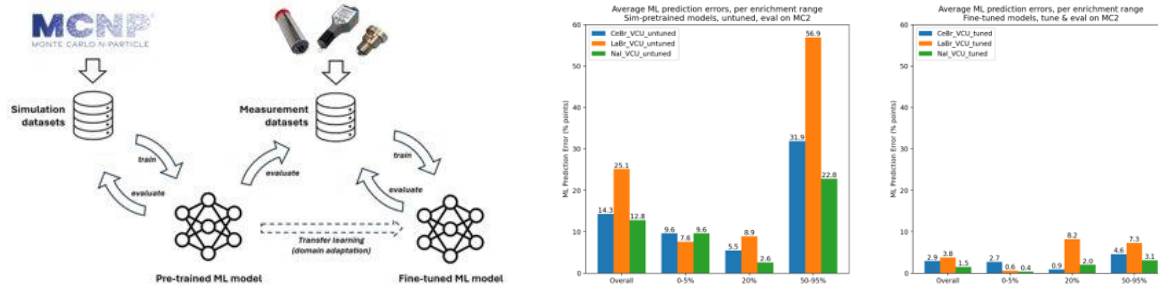
UNet baseline

Ours

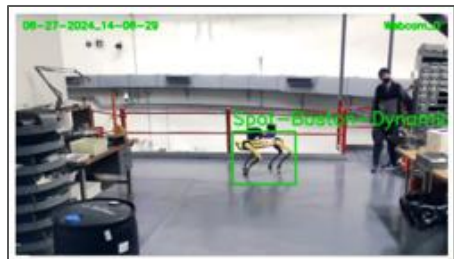


Robustly learning continuous scientific data with scalable conditional neural fields (*left*), physics-constrained diffusion models for x-ray coherent diffractive imaging (*above*).

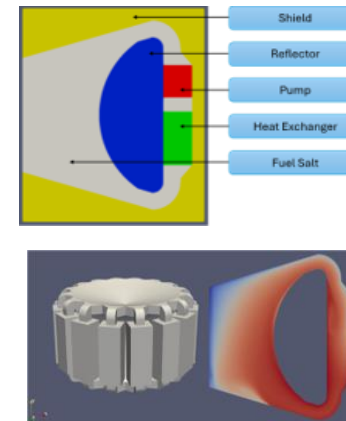
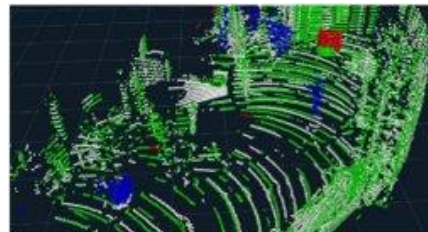
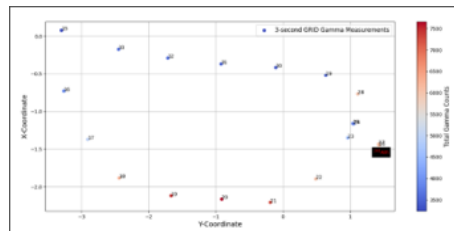
# Bringing AI into the Real World: Applications for security and safeguards



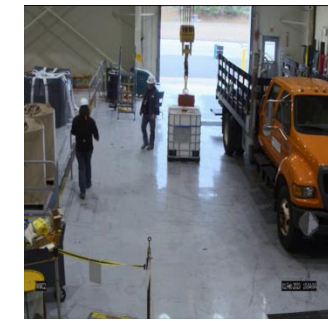
**Mixed-source ML training with domain adaptation**  
(uranium enrichment analysis)



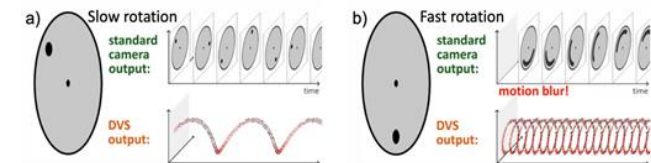
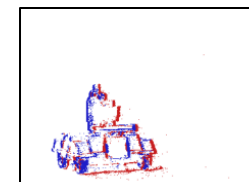
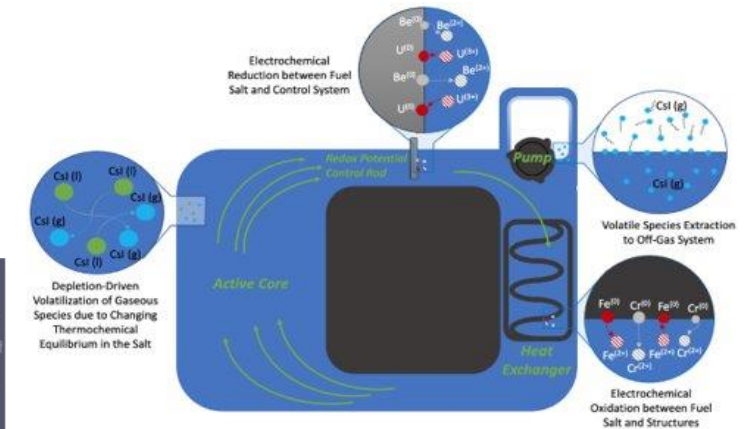
**ML-enabled autonomous robotic security missions**  
(camera verification, anomaly detection, and stray radiation detection in reactor facility)



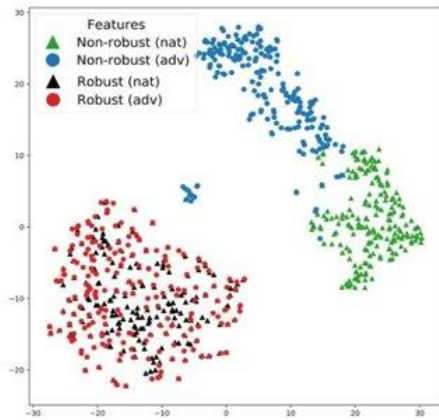
**ML with mixed-cost multi-physics modeling**  
(diversion detection of nuclear material in molten salt reactors)



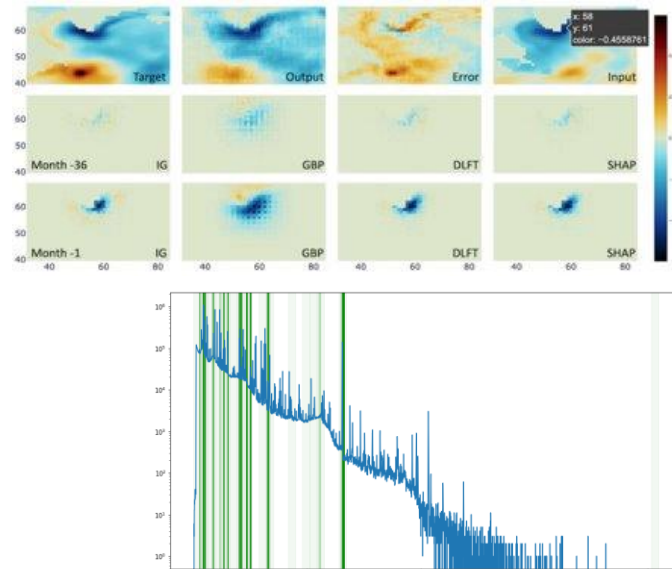
**AI-detection of manipulated images/video**  
(facility monitoring for arms control verification)



# Bringing AI into the Real World: Security and Trustworthiness of AI



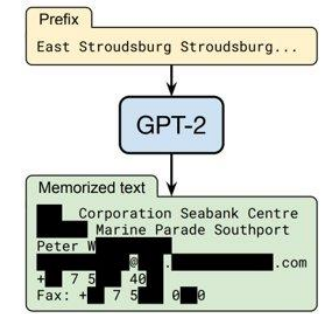
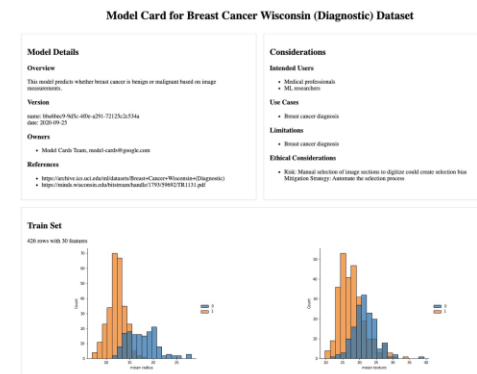
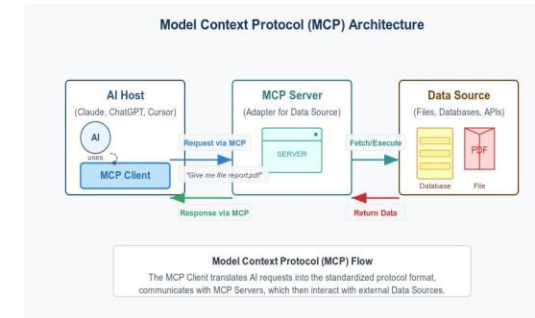
**Robust training of AI models to reduce susceptibility to adversarial attacks**



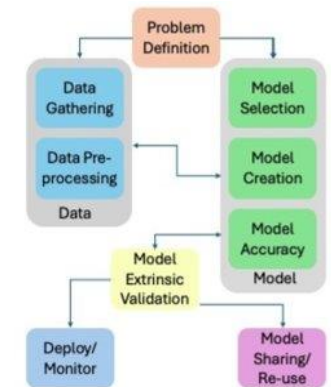
**Explainable AI** via e.g., feature visualizations, surrogate models, output interpretation.

**Interpreting LLMs/FMs:** neuron inspections, CoT traces, RAG and other external resources

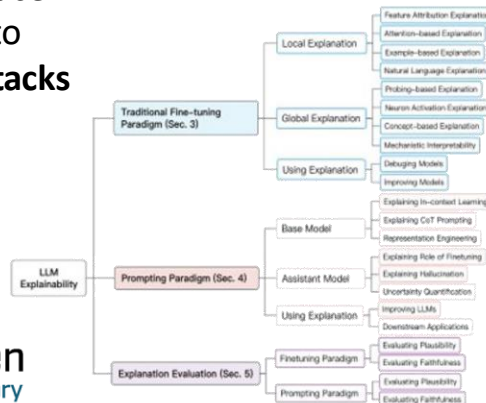
Adopting, implementing, and assessing **industry standards** (model cards, MCP, A2A, benchmarks, etc.)



Quantifying **data tainting, leakage, and poisoning risks** (e.g., for LLMs)



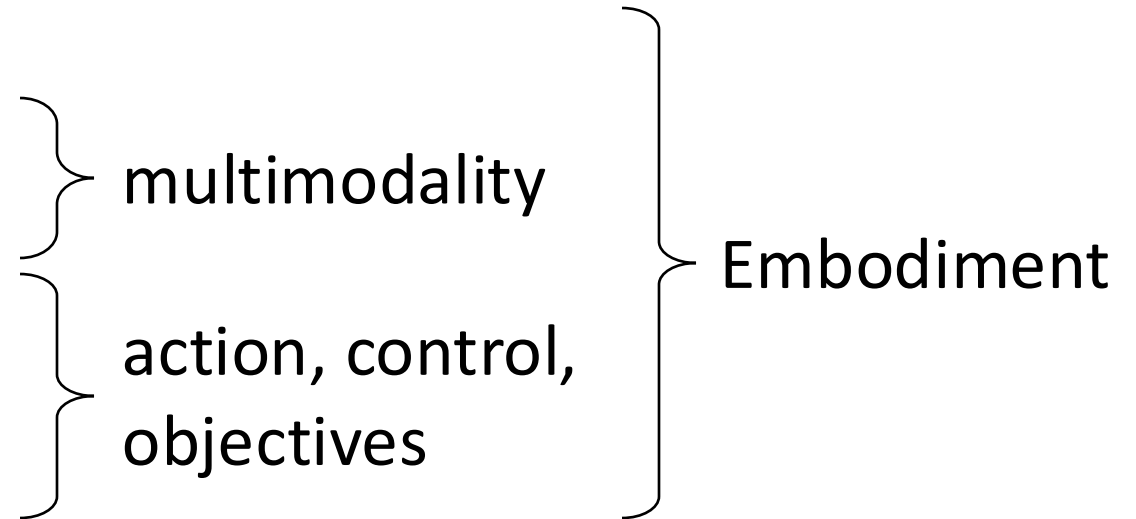
Identifying and mitigating **platform and lifecycle risks** for AI within larger ecosystems



# Embodied AI

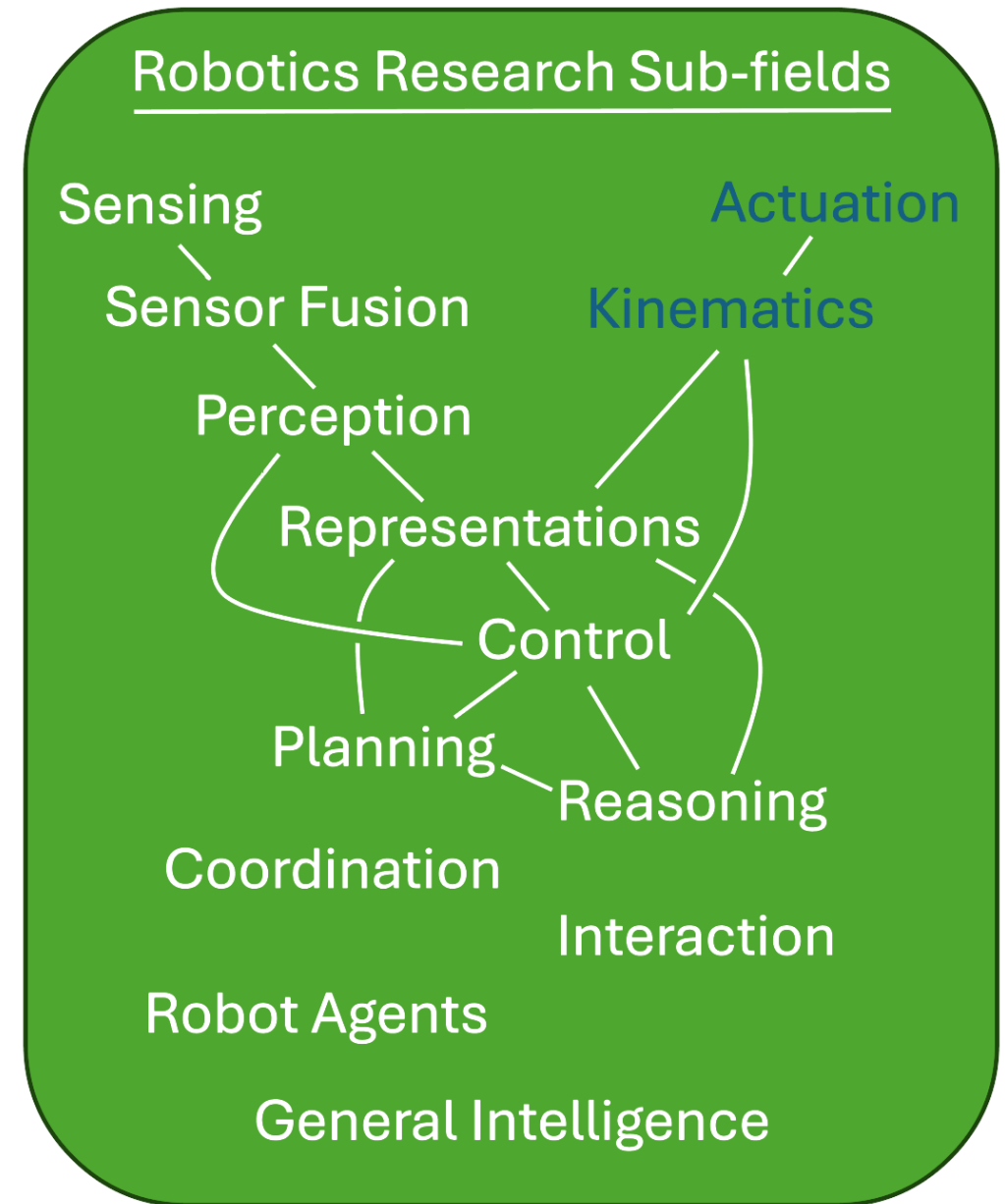
Physical extension of AI into an embodied, agentic form.

Agents that are situated in,  
perceive,  
learn about,  
respond to,  
act upon, and  
affect the **real world**



# Robotics Research

- Complex mixture of
  - Mechanical Engineering
  - Electrical Engineering
  - Computer Science
  - AI (CV, NLP, RL, etc)
  - Control Theory
  - Operations
  - Human factors
  - ...



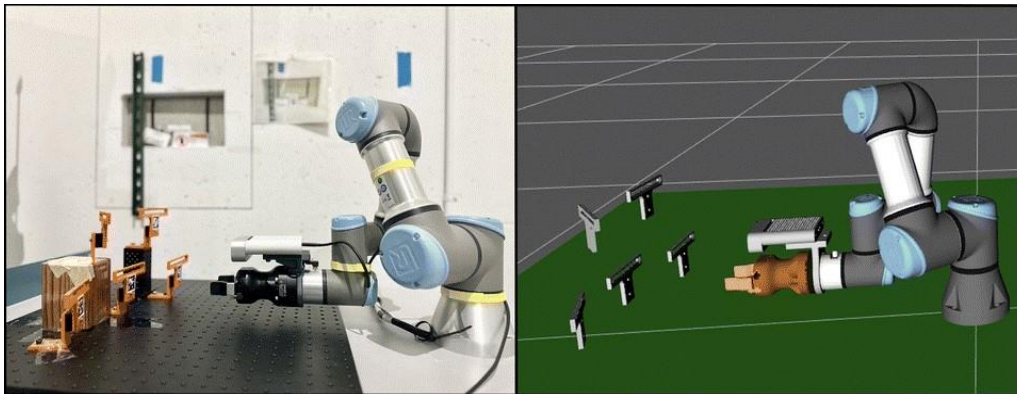
# Automation & Robotics at BNL

~20 automation and robotics platforms are being used and studied by groups across the lab

- Accelerate workflows
- Improve cycle consistency
- Mitigate hazards



Spot robot used for studying nuclear security applications at NN



Investigating robotic sample handling at NSLS-II



Automated Liquid Handling at CFN

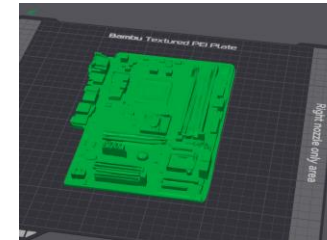
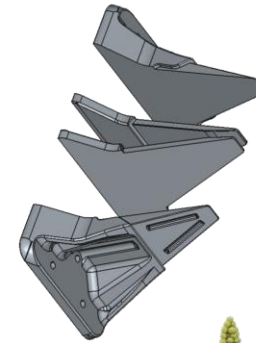
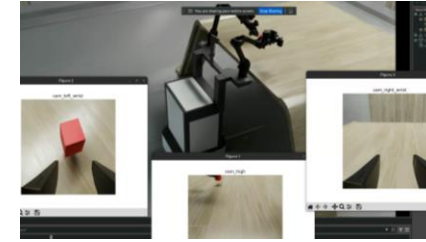
# AI for Robotics

- **Foundation Models** – AI models pretrained on massive data
  - Scaling laws
  - Generalization
  - Multi-modality
  - Emergent capabilities
- **AI Agents** – intelligent programs that persist, and demonstrate reasoning and planning to pursue objectives
  - Taskability
  - Tool use
  - Memory
  - Interaction

# *Scientific Embodied Agents Lab (SEAL)*

With initial ASCR ACT award and BNL PD support, we

- Established, equipped SEAL robotics lab
  - **Embodied AI** research with bimanual and humanoid robots
- Developed multiple working VLA training pipelines (on both **physical robot** and in **simulation**)
  - Developed and validated bimanual **dexterous manipulation** with 3D printed mockups
  - Also using decommissioned scientific parts/components for interaction



# Basic and Applied Research

*AI for advanced robotics, addressing current & future challenges*



## Basic Research

- Embodied AI
  - Novel Agentic AI and robotic FMs
- Broader AI/ML research
  - Spatiotemporal, multimodal, heterogeneous data for AI
  - Scaling AI models
  - AI/ML **robustness, security, and safety**
- Applied Math, Computer Science
  - Inverse problems, control theory, optimization, UQ
  - Middleware, simulations

## Applied Research

- AI Robotics Testbed
  - Spectrum of robotic **platforms, AI Models** and science **problems**
  - Scalable AI prototyping, development, evaluation
  - Unique, scalable **scientific action datasets and benchmarks**
- Dedicated intra-lab collaborations
  - Motivate novel AI with mission science, advance science with AI



# Resources, Communities, and Impact

- Resources & investments
  - Hardware, facilities, workforce
- Engaging within BNL
  - Workshops, demos, hackathons, etc.
- Industry, academia and other labs
  - Embodied AI Alliance
  - Synergistic inter-lab efforts
- Stakeholders and public
  - Communication plans with BNL Media
  - Testbed users, data and benchmark contributors (bidirectional benefit)

