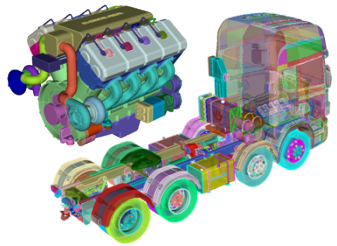
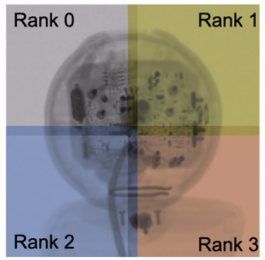
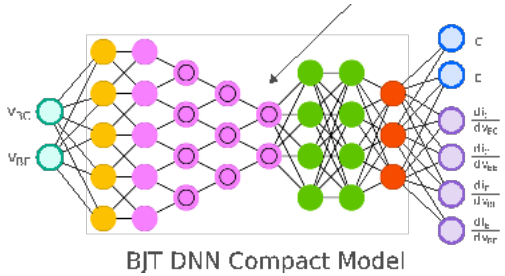
SAND2022-10920C

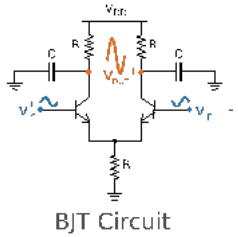
Sandia National Laboratories

AI for *Security*
NNSA's Role in AI4SES









Ron Oldfield
Manager, Scientific Machine Learning
Center for Computing Research

Presentation for 3rd Workshop on AI for Science, Energy, and Security

Bowie State University

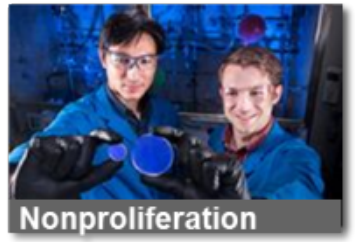
August 16—18, 2022

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

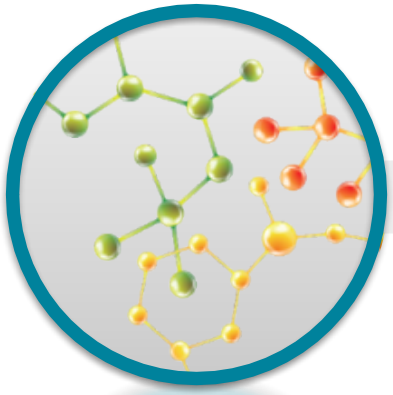
AI/ML has Great Potential for National Security Missions

Program	Mission Problem	Characteristics
Global Security	**Proliferation Detection and Characterization**	• Multi-modal sensors, distributed sensors, and real-time behavior • Physical models and ground truth may not exist • Real time monitoring with streaming data
Global Security	**Automatic Target Recognition for Military Applications**	• Limited data that is likely modified or disguised • Desire to reduce or remove human in the loop • Data available at multiple levels of sensitivity • Adversary withholds differentiating capabilities and tactics
Nuclear Deterrence	**Counterfeit and Aging Detection**	• Many sources of variation – unknown limits to what can be learned Lack of a mathematical foundation and physical models • Volume of data is very low
Nuclear Deterrence	**Large Scale Physics Experiments**	• Rich but sparse data - can be expensive to obtain • Multi-instrument, multi-experiment, multi-measurement • Uncertainty present in experiments and physics models
National Security Programs	**Analyst Support for Cyber and Intelligence Operations**	• Need to introduce AI without disrupting current operations • Very high consequence, very rapid transactions (many per minute) • Streaming data with very dynamic environment
Energy & Homeland Security	**Bioscience and Biosecurity**	• Multiple types of data requires data fusion • Data collection is often destructive • Theoretical models often don't exist
Advanced Science & Technology	**HPC System Management and Operations**	• Operations staff do not understand performance/failure mechanisms • Thousands of instrumentation points, but unknown if data provide useful insights • Complex resource usage makes it difficult to tune systems



AI-driven methods for designing, manufacturing and deploying products have the potential to revolutionize NNSA workflows

Discovery



New molecules and materials vital to national security priorities

- New polymers with customized properties
- High explosives with improved safety and performance
- Customized molecules for countering WMD

Design Exploration and Optimization

Major increases in efficiency and cost improvement

- Optimizing for robustness, performance and manufacturability
- AI enabled, non-intuitive solutions
- Ability to find optimal solutions over a broad parameter space

Manufacturing and Certification

Major advances in manufacturing efficiency and quality

- In-situ, defect detection and correction
- UQ approach to process and material certification
- Quantifying the value of experiments

Deployment and Surveillance

Characterizing behavior over the full life cycle

- Digital twin with aging effects
- Analysis of embedded sensors
- Predicting problems before they occur

NNSA aims to advance high-performance simulation, experimental and engineering capabilities, including AI/ML-enabled tools, to solve current and emerging national security challenges

ASC Advanced Machine Learning Initiative (AMLI) Strategy

The DDMD capabilities are supported by six capability-development areas identified in ASC Advanced Machine Learning Strategy.

Stockpile Drivers

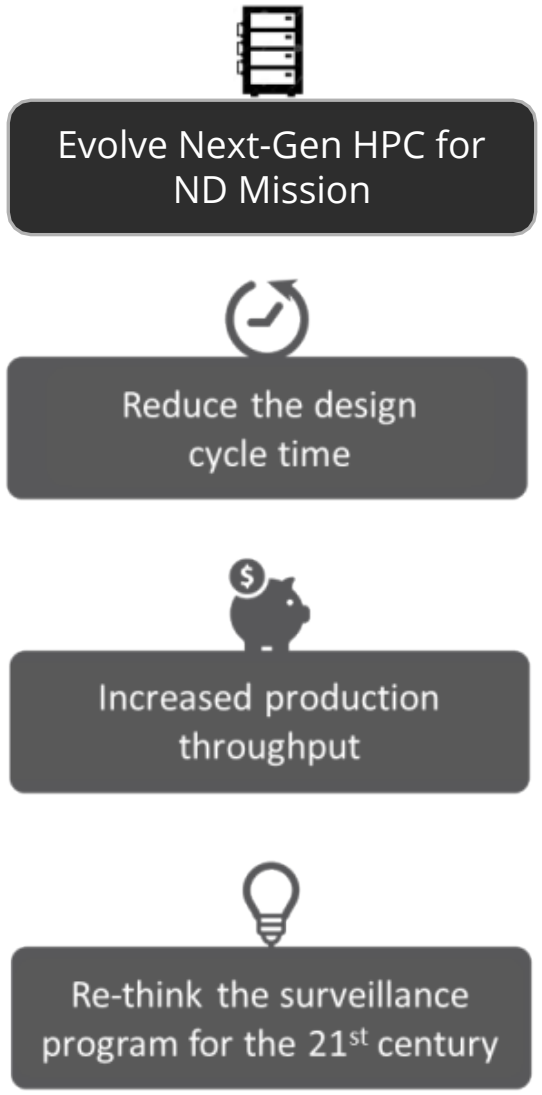
- Improved Efficiency in the Design Process
- Anticipatory Stockpile Decision Making

Science and Technology Drivers

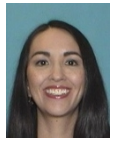
- Data-Driven Physics Models
- Enhance Experimental Design
- Reduce the Computational Cost of Physics Simulations

Six Capability Development Areas

1. Advance research in physics-constrained ML
2. Improve our ability to employ machine learning with sparse data,
3. Invest in validated and explainable machine learning,
4. Explore learning hardware systems in an HPC environment,
5. Create an AML-tailored data environment,
6. Improve simulation workflows, and
7. Build the machine learning expertise and workforce at the laboratories.



Example: Physics-Informed ML Material Models for Solid Mechanics



Sharlotte Kramer, Principal Member of Technical Staff, Experimental Solid Mechanics

P&EM

ATDM

Physics Constr

Sparse

Trust

Problem

- Traditional constitutive models incorporate first-principles and obey physics constraints, but have model-form errors too large for Nuclear Deterrence problems
- Purely data-driven models require large training sets, lack robustness, and are not generalizable
- Experimental data is emerging, but is sparse and is multi-fidelity (unusable for traditional and too sparse for data-driven)

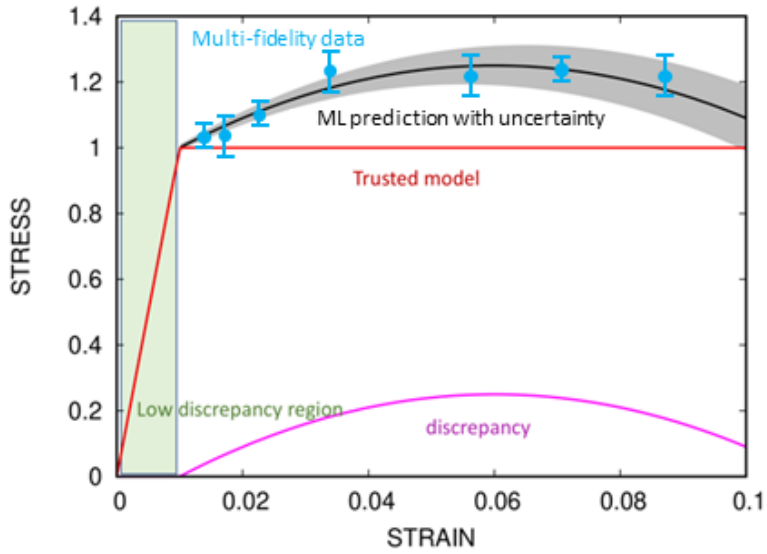
Technical Approach

- Use ML to correct model-form error in traditional modeling
  - Trained on fusion of multi-fidelity experimental data – maintains physical constraints, requires less data, includes uncertainty.
- Exemplars: Polymer foams and Additive Manufacturing metals

Deployment:

- Incorporation into SIERRA LAMÉ material library through partner P&EM projects

Key Partnerships: Amir Farimani (Carnegie Mellon University)



Example of the Traditional + ML-discrepancy Model Approach: Traditional elastic-plastic model plus data-driven discrepancy model with uncertainty is closer to multi-fidelity data.

Hamel, C. M., Long, K. N., & Kramer, S. L. (2022). Calibrating constitutive models with full-field data via physics informed neural networks. *arXiv preprint arXiv:2203.16577*.

Example: Credibility for Scientific Machine Learning:
Training Data Verification and Model Qualification

PI: Erin Acquesta, Principal Member of Technical Staff, Computational Decision Science

V&V

ATDM

Sparse

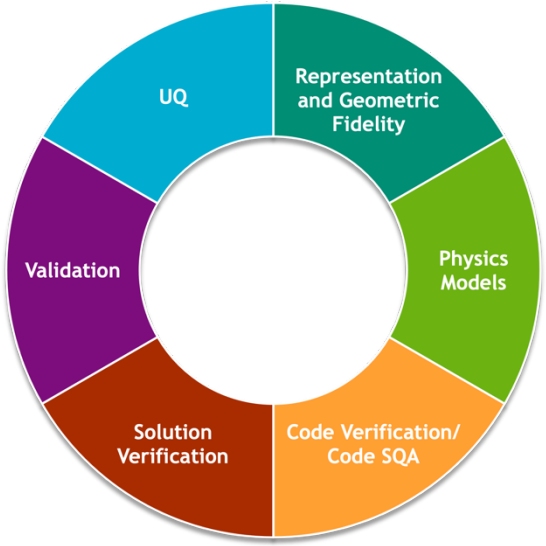
Trust

Data Env

Workflow

Problem

- High-consequence ND workflows require **rigorous Verification and Validation (V&V)** and Uncertainty Quantification (UQ)
- Need evidence-based credibility for scientific machine learning when used in ND workflows.

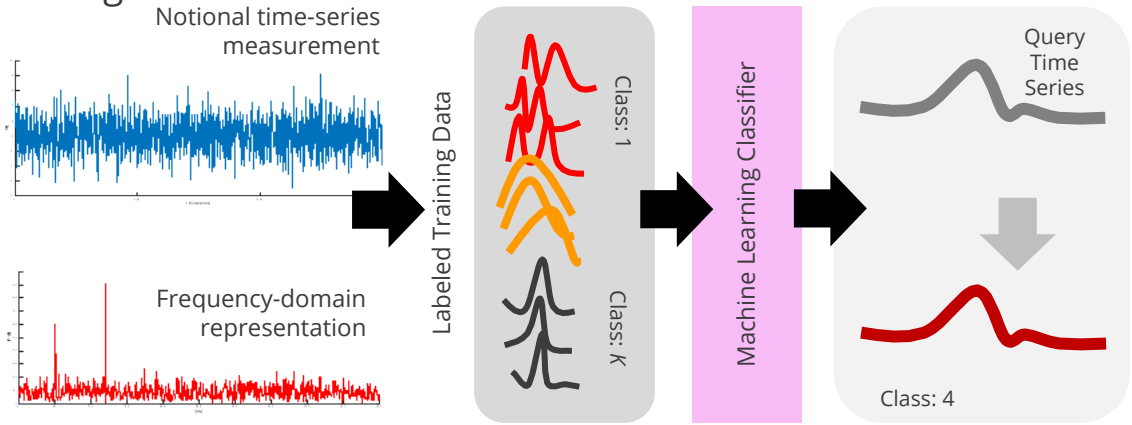


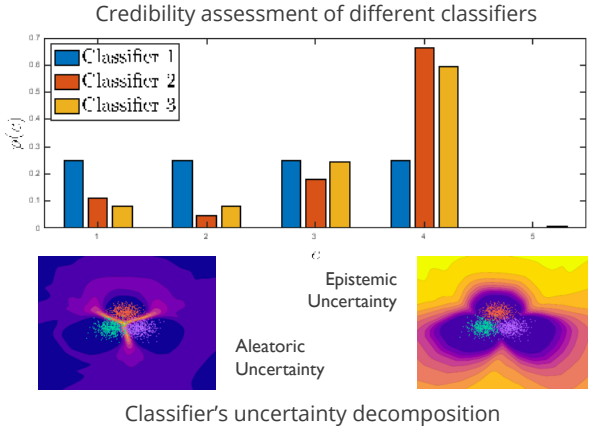
Technical Approach

- Leverage CompSim and traditional ML credibility workflows into a tailored SciML framework.
  - Predictive Capability Maturity Model (PCMM), Datasheets for Datasets
- Exemplar: Device Aging Classification
  - Predict health of devices using waveforms collected using non-destructive tests.
  - Identify key input features in time or Fourier domains, assess the quality of training datasets, and decompose uncertainty into its aleatoric and epistemic components.

Deployment:

- Targeted integration into Dakota and other ASC tools





Classifier's uncertainty decomposition

Security is an important piece of the DOE AI Mission

NNSA's national security mission has somewhat unique requirements (e.g., rigorous V&V) but **many aspects of foundational research are similar** to the open science community

Partnership with ASCR, Vendors, Universities and others will be key to ASC's strategy

- We simply cannot do this on our own – we already leverage billions in investments from industry
- We also cannot simply adopt technology thrown "over the fence" and expect it to work effectively

ECP provides a model for how ASC and ASCR can collaborate openly within constraints of a classified mission space

- It took years to develop a productive ECP collaboration model, we should build on that experience

Outcomes of the AI4SES Workshops will likely influence future NNSA investments in AI/ML to address Grand Challenge problems in National Security

- It is vital for the US to tackle hard problems, build the enabling tech, and train a workforce capable of rapidly addressing future/unforeseen challenges.