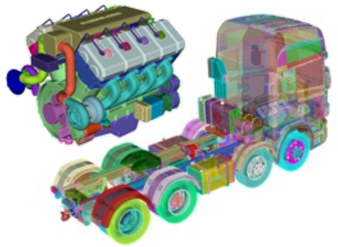
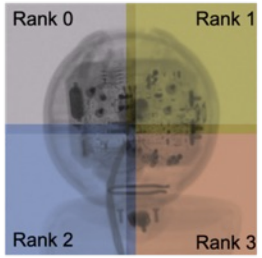
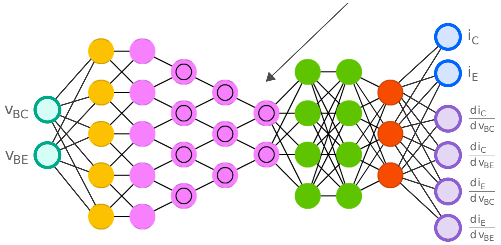
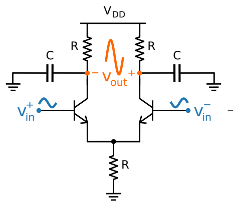
Scientific ML for National Security







BJT DNN Compact Model



BJT Circuit


Ron Oldfield
Manager, Scientific Machine Learning
Center for Computing Research

PSAAP IV Planning Meeting

Houston, TX

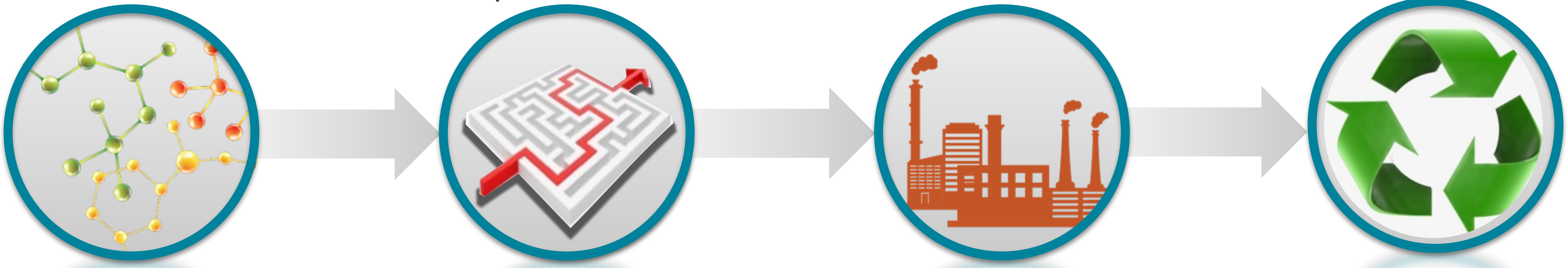
August 2023

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.

SAND2023-07518PE

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

Discovery | **Design Exploration and Optimization** | **Manufacturing and Certification** | **Deployment and Surveillance**



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

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

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

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.

Evolve Next-Gen HPC for ND Mission

Reduce the design cycle time

Increased production throughput

Re-think the surveillance program for the 21st century

Example: Credibility of SciML for NNSA Missions

Purpose

The NNSA Labs emphasize credible-trustworthy scientific ML (SciML) as a necessity for it to meet national security mission delivery.

Motivation

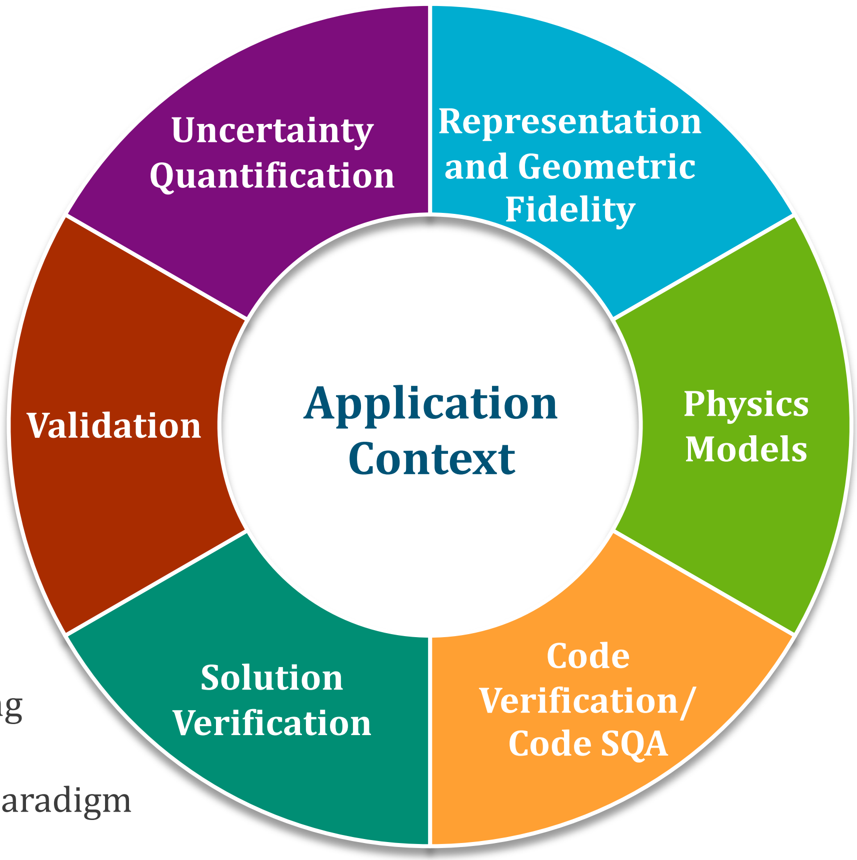
While ML holds great potential for mission critical applications, evaluating the credibility of current techniques poses challenges that may hinder its widespread acceptance and use.

The NNSA Labs must strike a balance between leveraging the advantages of ML while ensuring its responsible use for national security purposes.

PCMM: Predictive Capability Maturity Model

The computational simulation (CompSim) credibility process assembles and documents evidence to ascertain and communicate the believability of predictions that are produced from computational simulations.

Evidence Basis
- Plan
- Execute
- Organize & Analyze



Elements
- Categories for collecting evidence
- Dependent on model paradigm

Communication
- Peer Review
- Plausible Prediction Bounds

CompSim Model → Prediction

Application Context
- Partial Differential Equations, PDEs
- Computational Fluid Dynamics, CFD

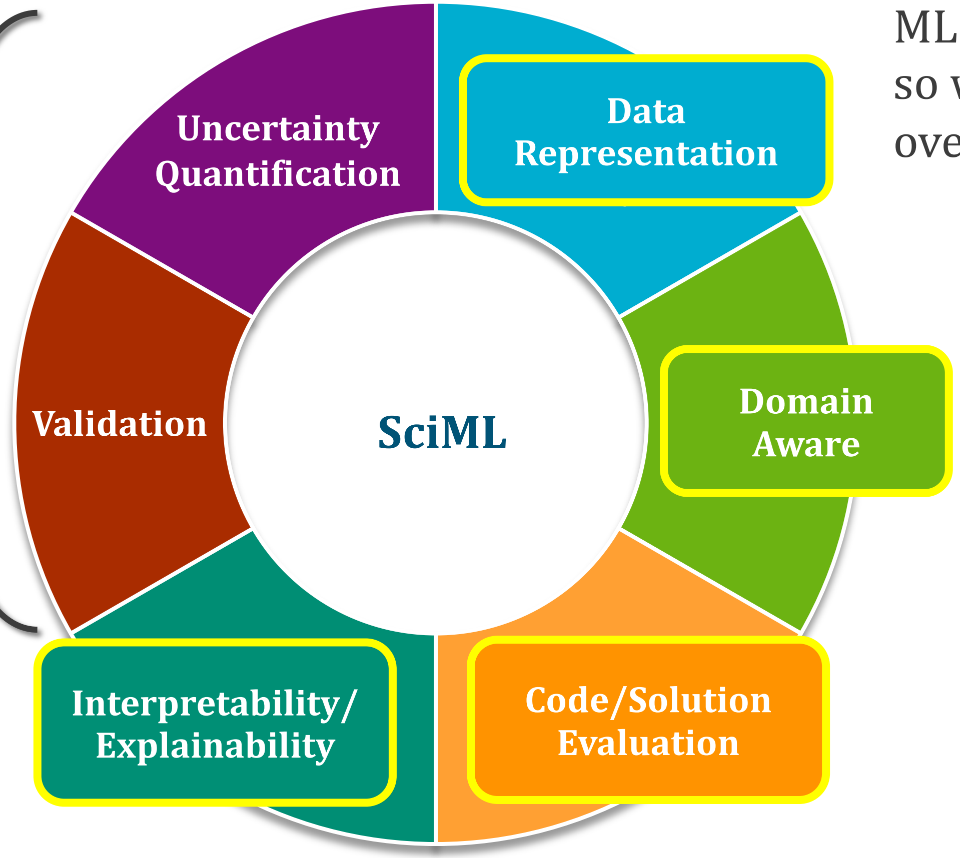
Our work builds upon NNSA's 20+ years of experience in verification, validation, and uncertainty quantification (VV/UQ) for complex problems with limited data. PCMM evolved from industry standards and lab/academic collaboration.

"Predictive Capability Maturity Model for Computational Modeling and Simulation" by Oberkampf, W.L., Pilch, M., and Trucano, T.G., SAND2007-5948

Developing a Credibility Model for Codes with SciML

Credibility process assembles and documents evidence to ascertain and communicate the believability of predictions that are produced from computer models.

UQ and Validation are currently the core areas of research that exists for ML credibility.



ML models learn patterns from data, so we prioritize data representations over the geometries.

ML is applied more broadly and it is not only physical principles we want to preserve.

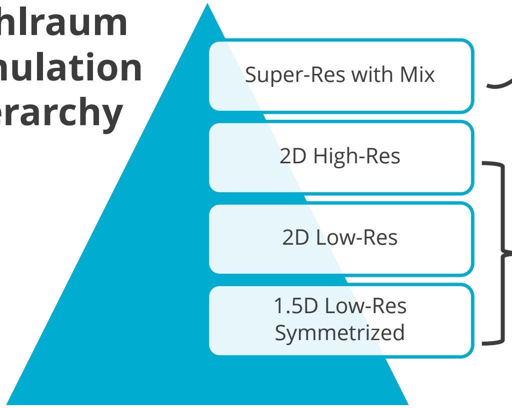
Verification asks "are we solving the equations correctly", ML models do not start with equations. We may want to reconsider the terminology for ML and address more of the community of practice methods.

A credibility model for codes that use SciML is essential to ensure confidence in our model predictions.

Ron Oldfield, Sandia National Laboratories

Example: Multi-fidelity simulation surrogates are used to maximize cost/benefit for large design space exploration

Hohlraum Simulation Hierarchy

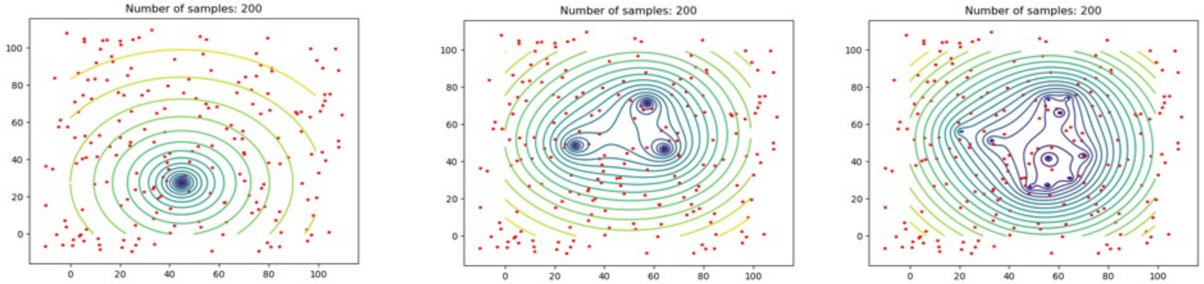


Need designs to perform up here

But we can only afford down here

Searching 30+ parameters!

Effective sampling and advanced surrogate models better capture design space



Every simulation requires millions of atomic physics calculations – major computational cost!

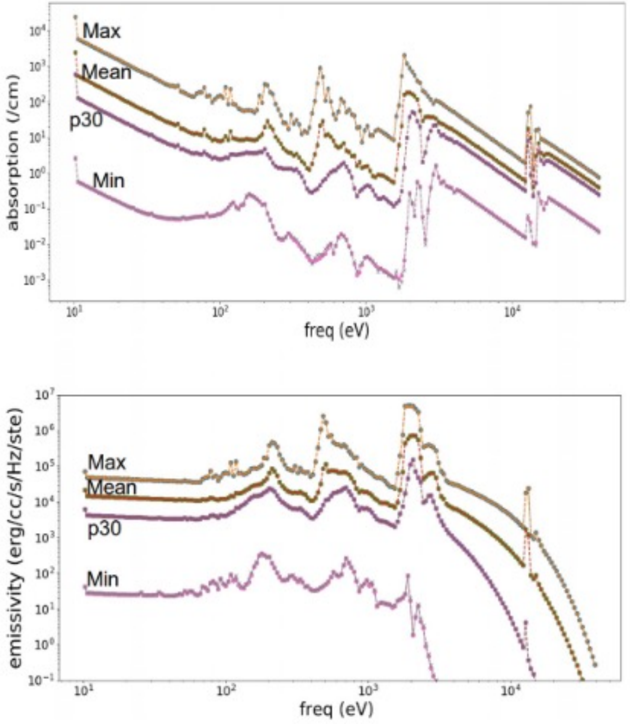


FIG. 6. Results of the *DNN* (crosses) compared to *Cretin* (rounds). Absorption coefficients on the top and emissivities below. For each bin, we show the maximum, mean, percentile 30, and minimum values on all the test datasets.

A Deep Neural Network (DNN) trained using high fidelity atomic physics calculations provides a ~10x speedup with high accuracy.

Physics of Plasmas **27**, 052707 (2020); https://doi.org/10.1063/5.0006784

Lawrence Livermore National Laboratory

U.S. DEPARTMENT OF ENERGY

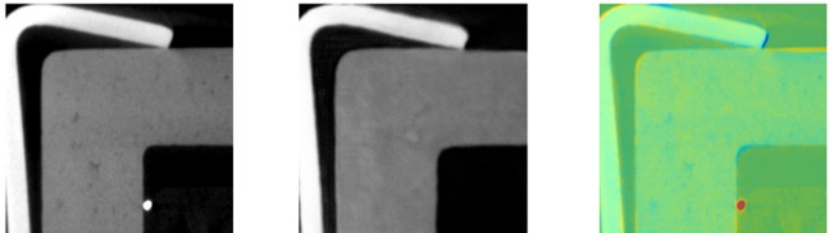
National Nuclear Security Administration

ASC

Example: Digital Twins for Manufacturing and Certification

Sparse Data

- Small quantities of unique parts
- Expensive builds and experiments
- ML confidence on sparse data and setting bounds on how many data points are required for a given confidence / uncertainty quantification
- Bayesian Optimization
- Supplementing sparse data with simulation data – combining simulation and experimental data

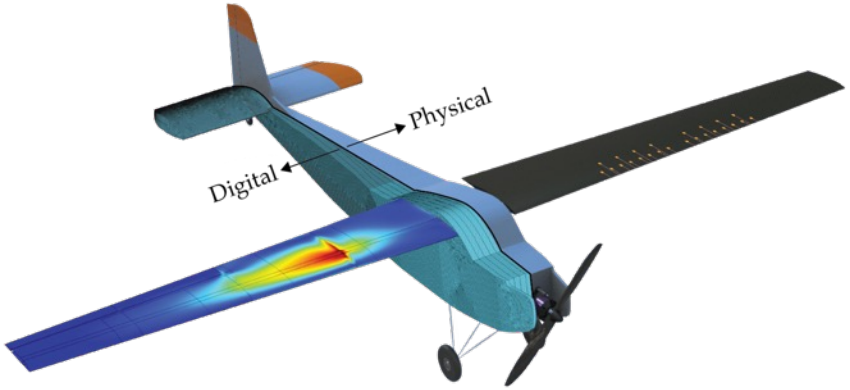


Example of anomaly detection on a current transformer corner using a trained AnoGAN.

Donahue, Emily A., et al. "Deep learning for automated defect detection in high-reliability electronic parts." *Applications of Machine Learning*. Vol. 11139. SPIE, 2019.

Automated Inspection

- Real time AI-assisted defect screening
- Using AI/ML to characterize manufactured parts
  - Radiography, computed tomography, in-situ monitoring, metrology, etc.
- Simulations of as-built devices
  - Characterize behavior
- Design and production working together –



Artificial Intelligence for the prediction & control of complex systems
Karen Willcox, UT Austin

Deployment and In-Situ Surveillance

- simulations and digital twins

Additional Areas of Interest (just a couple)

Large Language Model (LLM) Advancements

- LLMs can be tied directly to documentation, reports, etc.
- How can LLMs be applied to scientific data?
- Will LLMs be used to direct the computation simulation workflows of the future?
- What can we do with smaller datasets, when we don't expect the model to perform as many tasks?
- How and where can transfer learning be employed? How can the technique of self-attention be employed for improved transfer learning?

Hardware, Data, and Workflows

- Innovative hardware designs that support a mix of high-fidelity modsim and AI/ML
- Applications to inform hardware and software stack evaluations
- Innovative approaches to data management and sharing
- Innovative workflows and approaches to large-scale optimization (for design)

SciML for National Security has many Open Challenges

Six Capability Development Areas Identified in AML Strategy

- Research in physics-constrained ML,
- Employ machine learning with sparse data,
- Validated and explainable machine learning,
- Explore learning hardware systems in an HPC environment,
- Create an AML-tailored data environment,
- Improve simulation workflows

https://www.anl.gov/ai-for-science-report

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

Contacts and Credit

Special thanks to the following for providing content:

Credibility for SciML

- ***Erin Acquesta***, Sandia National Laboratories, eacques@sandia.gov
- ***Bill Rider***, Sandia National Laboratories, wjrider@sandia.gov

Multi-Fidelity Surrogates for Design Space Exploration

- ***Katie Lewis***, Lawrence Livermore National Laboratory, lewis66@llnl.gov

Digital Twins for Manufacturing and Certification

- ***Nathan DeBardeleben***, Los Alamos National Laboratory, ndebard@lanl.gov
- ***Cari Martinez***, Sandia National Laboratories, cmarti5@sandia.gov

Summary and Strategy and PSAAP POC

- ***John Feddema***, Sandia National Laboratories, jtfedde@sandia.gov

… and to the many staff and management that contributed to the AML Strategy!