Bernie AI & Beyond

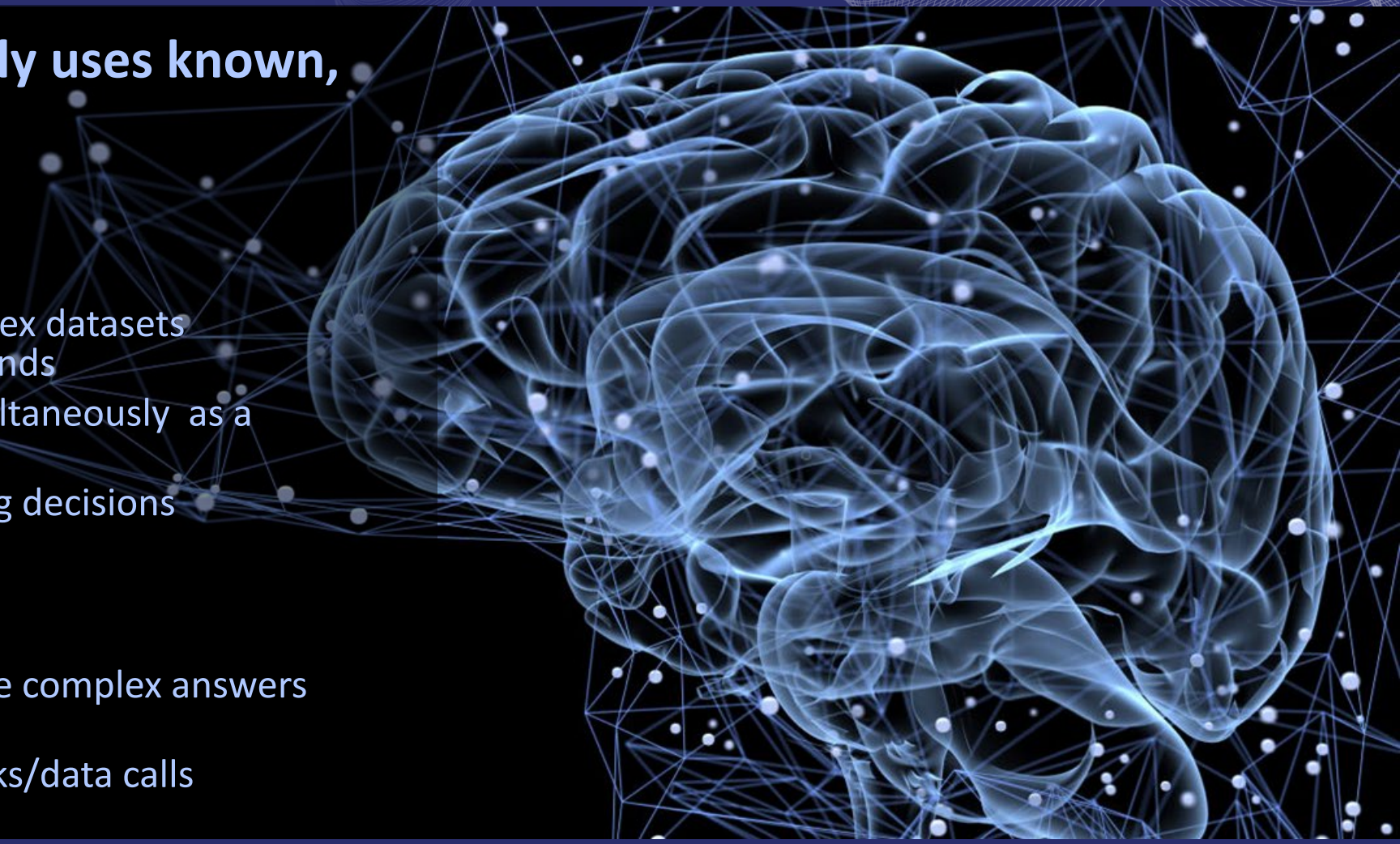
National Nuclear Security Administration (NNSA)
Yousseff Abed, Lawrence Livermore National Laboratory (LLNL)
Bernie AI Lead and BUILDER Project Manager

Julie B. Krebs, NNSA HQ Operations & Maintenance Division (NA-914)
NNSA BUILDER Program Manager

Imagine Artificial Intelligence as a future capability

That safely and securely uses known, verifiable NSE data to:

- **Guide** prioritization
  - Analyze large and complex datasets to identify data risks/trends
  - Evaluating projects simultaneously as a "difference engine"
  - Aiding impartial planning decisions
- **Respond** to requests
  - Providing simple or more complex answers for user convenience
  - Automate repetitive tasks/data calls

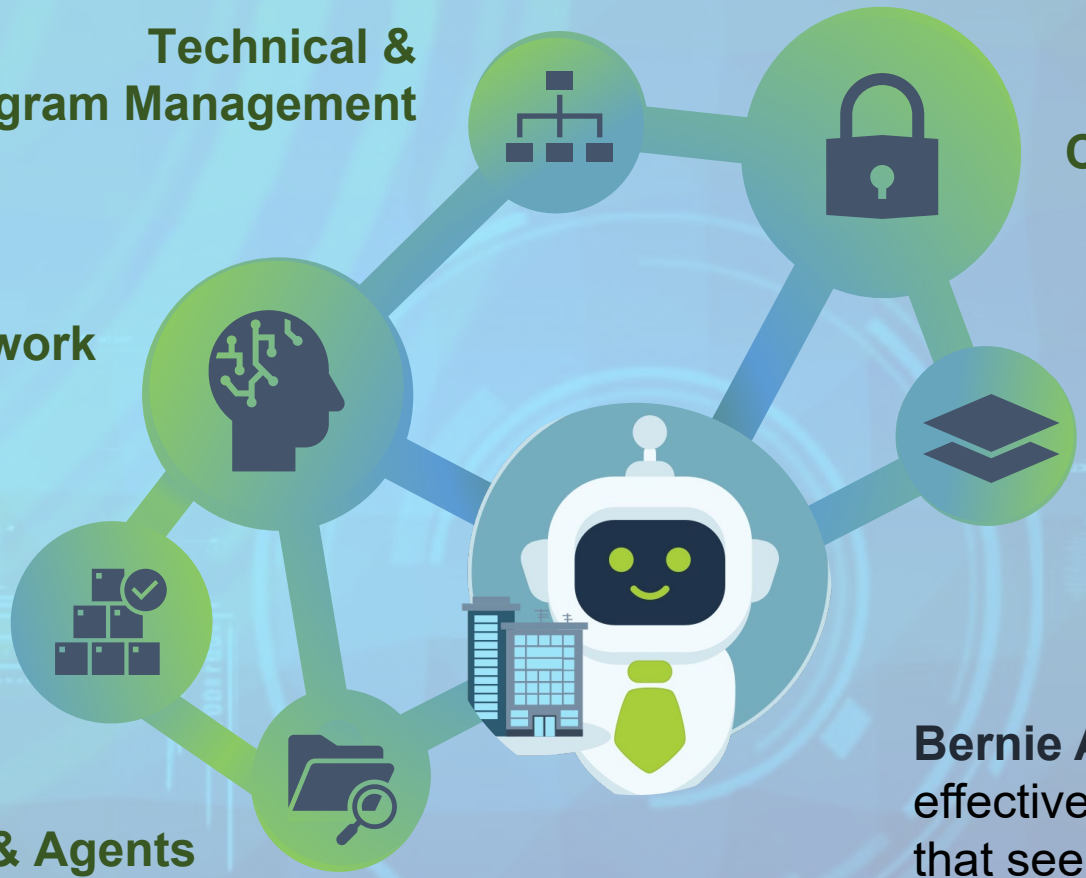


Imagine accelerating mission using “AI for good”

Using a proactive and interactive tool with total asset visibility, that:

- **Identifies** risks
  - Flags data anomalies
  - Predicts equipment failure
  - Tests assessment methodologies
- **Solves** problems
  - Improves correlation of RPV and construction costs
  - Find better life extension opportunities
  - Maintain knowledge easing succession planning

Bernie AI Team Approach



Bernie AI: an AI/ML tool that facilitates more effective, efficient, and timely decision-making that seeks to enhance rather than replace human judgement

The Bernie AI Team

Julie Krebs
Program Leader

Yousseff Abed
Technical Leader

Cliff Shang
Analysis. Leader

Mitchell Haraburda
Program Analyst

Alan Deng
Portal, Frame Works

Cebastian S. Hernandez
LLM Architect, Developer

Mazie Mauricio
Portal, UI/UX, Graphics

Michael Archibeque
Training, Agents, Modeling

Kate Heller
Technical Communications

AJ Fontana
Data, Agents, Training, Modeling

Cassie Tucker
Cyber Security, Analysis

Pilot Investigative Areas

LLM & Framework

- Choose hardware, LLM, plugins, vector database
- Determine cost, sustainability, portability
- Retrieval-augmented generation

Cyber Security

- Lead Red Teaming, M&O and NSE views
- Determine question redirects
- Mosaic effect prevention

Data Pipeline & Agents

- Determine agents, where data resides, APIs needed
- Improve responses
- Ensure data governance

R&D Modeling Team

- Enlist community help
- Release verification tools, portal, Q&R library
- Train and fine-tune

Small and Large Language Models

SLM Best Uses

- Specialized knowledge
- Efficient and low-latency
- Mobile applications
- Voice assistants
- IoT devices
- Educational purposes

Microsoft's PHI-2 and Mistral 7B are high-quality sources similar to LLMs.

VERSUS

LLM Best Uses

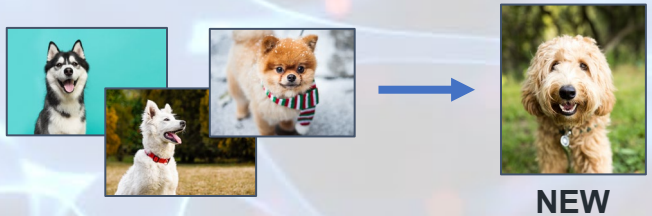
- Broad knowledge
- Long training window
- High-precision
- Generate human-like text
- Research applications
- Multimodal abilities

Llama Index and Langchain are frameworks for LLMs.

Primary AI Model Types

	Generative AI *is a creative author of new content, ideas, and images drawing inspiration from existing datasets*	**Predictive AI** *is an analytical detective able to identify patterns, make predictions, and classify existing data*
Objective	*Create new data*	*Classifies existing data*
Type of Learning	*Probabilistic modeling*	*Discriminative modeling*
Task management	*Unsupervised*	*Supervised (ideal for a secure dataset)*
More accurate results	*Includes outlier data*	✓ *Doesn't include outlier data*
Faster to train		✓
Greater ability to trend and make predictions		✓
More effective with data that isn't uniformly categorized	✓	
Requires more computational resources and vast training data	✓	

Trained Dataset → **Result**



NEW

Cat | Dog

CATEGORIZED

Choosing Predictive AI

Predictive and Generative AI are different; generating new data is not desirable

Weighing Predictive AI Pros & Cons

PROS	CONS
Pinpoint Customer Behavior	Heavily Relies on Trained Data
Enhance Customer Experience	Data Security Concerns
Make Informed Decision	Expenditure*

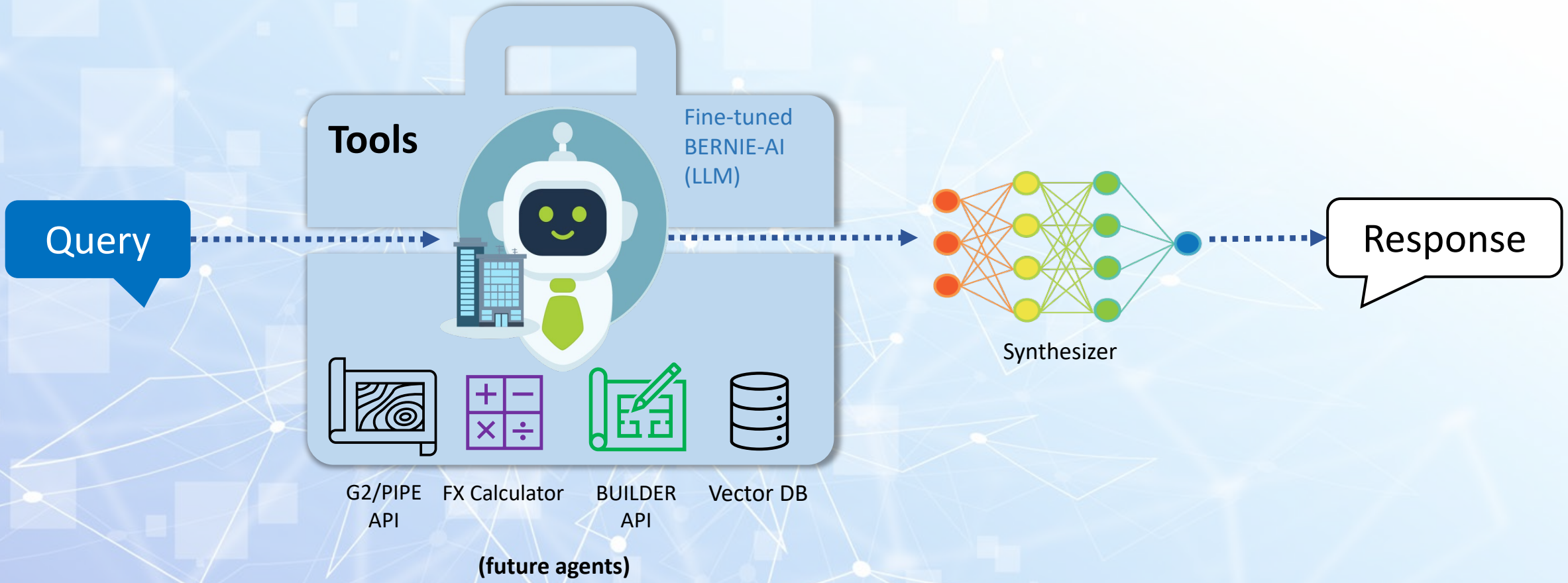
**Considering the necessary of hiring experts with specialized skills for data collection, cleaning, analysis, and other operations, which increases costs*

Conscious and Conscience

A user portal designed to combat AI hallucination

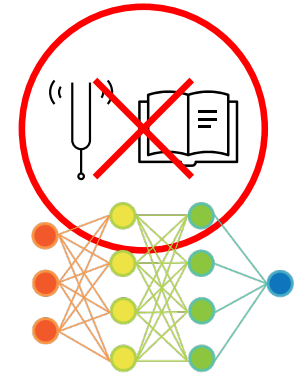
- Direct access to Bernie AI team
- Validation using documents & data
- AI Training feedback loop
- Developer blogs
- Community of practice resources
- Research links

Agents Bring Forward Key Data



Importance of Red Teaming

To build a safe AI, a key requirement is building a robust and efficient red teaming process

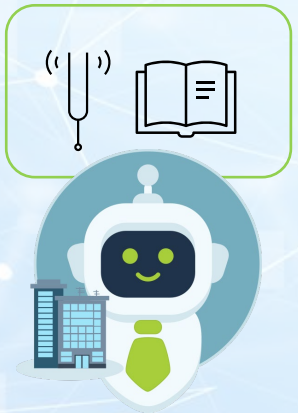


Open-source LLM

"How to make a cake?"

"Just buy a cake from the store"

VERSUS



Bernie-AI LLM

"How to make a cake?"

"Sorry I am only able to response to Infrastructure data"

Systematically probing the LLM to identify vulnerabilities, biases, and potential misuse cases

Schedule for 15-Month Bernie AI Pilot Program

FY24 Q3

- *Define pilot project scope*
- **Cybersecurity review**

FY24 Q4

- *Form focus group*
- *Collect customer input*
- AI framework paper
- Develop documentation
- Implement IT resources

FY25 Q1

- Develop initial LLM training plan
- Implement initial plan
- Future cybersecurity conditions paper

FY25 Q2

- Proof of concept using APIs with current apps
- Connect to multiple data sources
- Implement training program
- Develop an enterprise data acquisition plan

FY25 Q3

- Question review
- 12-month evaluation
- Develop expanded LLM training scope
- Complete model programming
- Implement enterprise data acquisition plan

FY25 Q4

- **Deliver evaluation results June 2025**
- State of neural network paper
- Add neural network layers
- Investigate additional input and output appliances

Questions?

Julie B. Krebs, NNSA BUILDER Program Manager
Julie.Krebs@nnsa.doe.gov; **Best Method to Reach POC**
Mobile: (505) 382-4410
Working from home in Albuquerque, NM