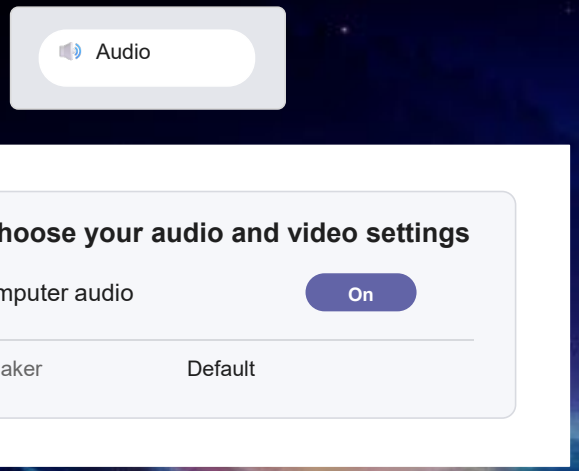
# Welcome to the Working Group Meeting

## We will begin at 2:00 PM E.T.

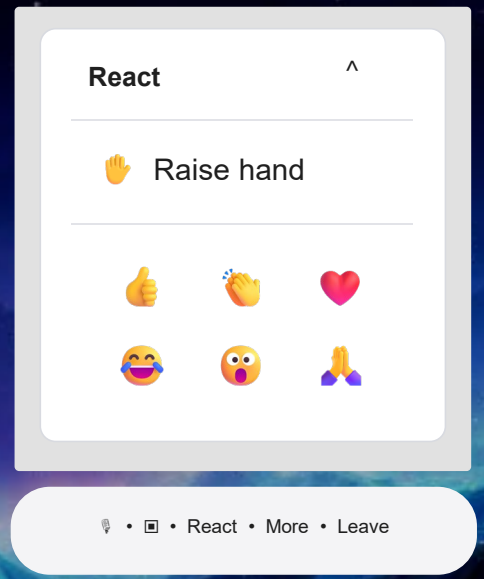
OPEN POWER AI CONSORTIUM

Join using computer audio. Confirm the speaker and microphone shown in the pre-join screen, then select "Join now."

Your microphone may be muted by the host.

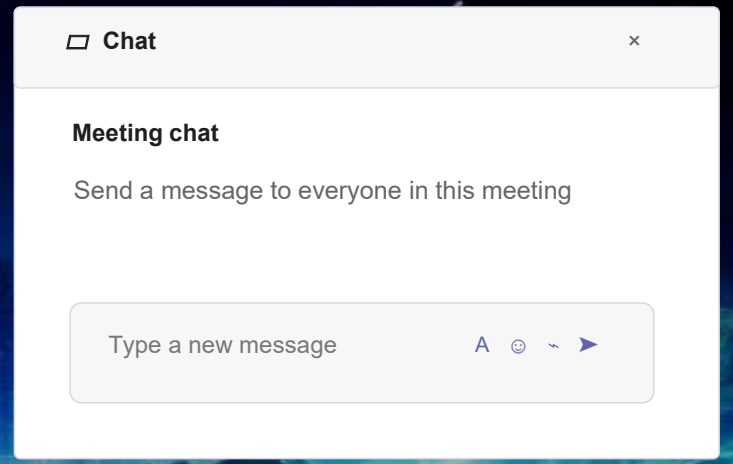



Would you like to contribute or ask a question verbally? Select "React," then choose "Raise hand." A presenter will call on you.




You can submit a written question at any time through the meeting Chat.

Please send your message to "Everyone in this meeting."




In the chat, introduce yourself with your name, company, and your role.

***Reminder: This meeting is being recorded***


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# OPAI Deployment and Implementation Working Group

## November Working Group Meeting

Jason Hollern
Technical Executive
Open Power AI Working Group Leader

November 11, 2026



© 2026 Electric Power Research Institute, Inc. All rights reserved.

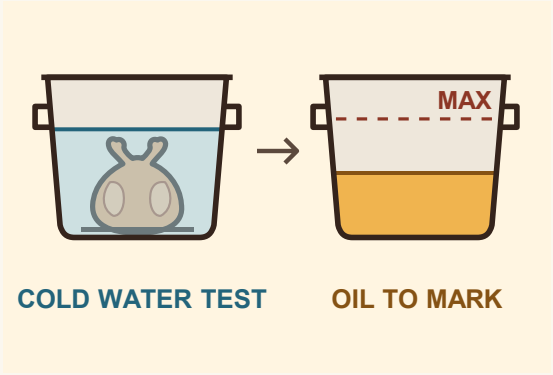
# AGENDA

- Safety Message
- Deployment/Implementation WG Updates
- Cyber Security AI Use-Case Implementation
  - Jeremy Lawrence, Hardware Accelerated Security at the Edge (HASE)
- Oral History AI Use-Case Implementation
  - Avery Hodges, Walz Oral History Application
- Open Discussion
- Adjourn

# Thanksgiving Turkey Fryer Safety

OUTDOOR PROPANE FRYERS

## 01 Set the oil level



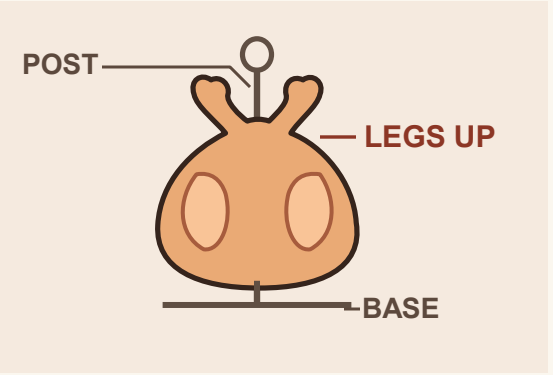

Use your fryer's fill line.
No line? Cover bird with water.
Lift bird out. Mark waterline.
Drain and dry. Fill to mark.

## 02 Thaw and dry



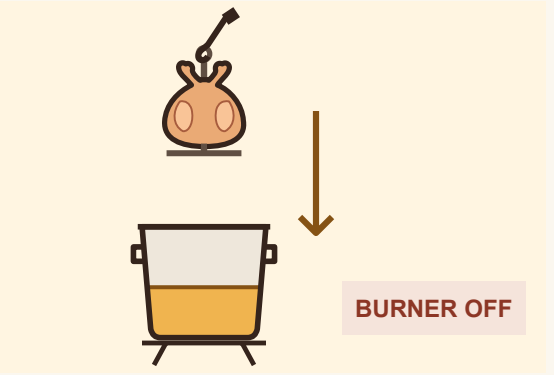

Thaw completely in the fridge.
Pat dry inside and out.

## 03 Mount the turkey




Slide bird over the rack post.
Rest it on the base, legs up.
Follow your model's rack setup.

## 04 Lower it slowly




Turn the burner off first.
Wear heat-resistant gloves.
Hook the ring. Lower slowly.
Pause if oil bubbles up.

## DO

- Use level ground outdoors, 10+ ft from buildings.
- Stay with the fryer and watch the oil thermometer.
- Keep kids and pets 3+ ft away.

## DON'T

- Fry on a deck or under a roof.
- Overfill the pot or drop the turkey.
- Move the fryer while the oil is hot.

**⚠ OIL FIRE? Back away and call 911. Never use water.**

# A Salute to US Veterans





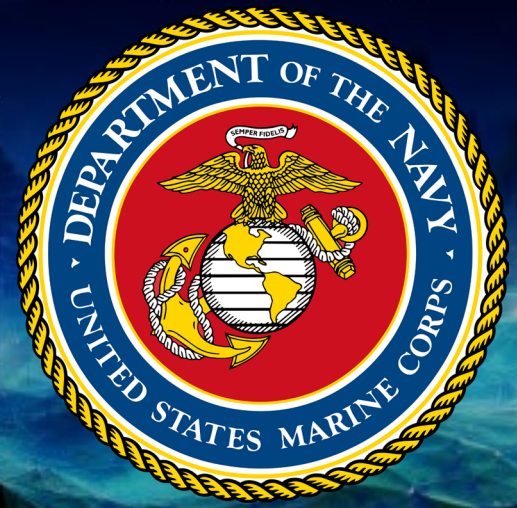








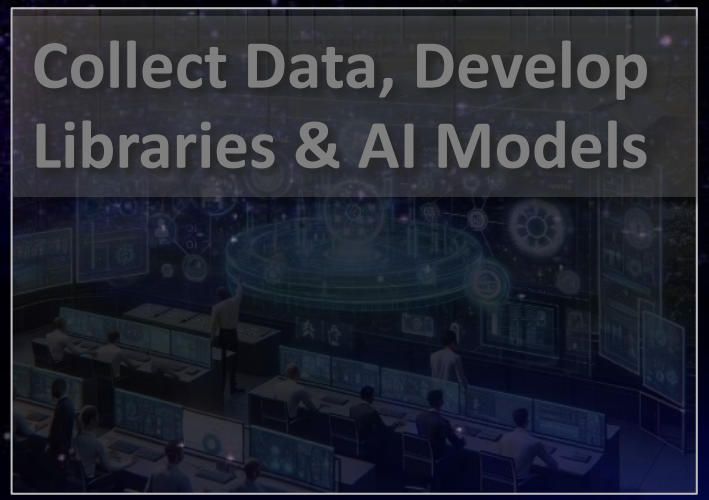


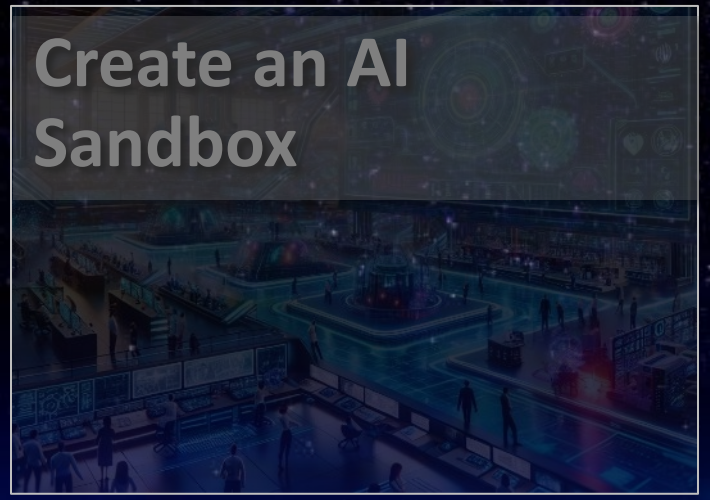





© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Open Power AI Consortium – Key Objectives







## Implementation and Lessons Learned

- Collaborate with leading AI developers to deploy AI models.
- Develop a feedback loop from deployments for refinement and optimization.
- Maximize impact via knowledge sharing among consortium members.


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Implementation Workstream Goals & Desired Outcomes

1. Connect commercially available AI solutions to end-users
2. Transfer, pilot, and implement new use-case solutions to industry
3. Foster a collaborative environment to improve the AI value proposition
4. Collect lessons learned through applications, demonstrations, and scaled implementation
5. Develop AI implementation guidance to help companies with successful implementation and value realization


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Three Main Thrusts to Accomplish Goals

## Research Products

- Value: Learning from implementation opportunities



## Outreach and Interactive Knowledge Transfer

- Value: Interactive collaboration and awareness
- Value: Presentation opportunities



## AI Tool Implementation

- Value: Experience with AI tools and streamlined implementation
- Value: One-on-one and community use-case build out




© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Upcoming Events

## 2026 Open Power AI Events

### January

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |

### February

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| | | | | | | |

### March

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | | | | |

### April

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | | |

### May

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | | | | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | | | | | | |

### June

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | | | | |

### July

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| 26 | 27 | 28 | 29 | 30 | 31 | |

### August

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | | | | | 1 |
| 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 16 | 17 | 18 | 19 | 20 | 21 | 22 |
| 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 30 | 31 | | | | | |

### September

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 | 30 | | | |

### October

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 |
| 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 |

### November

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | | | | | |

### December

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 | 30 | 31 | | |

- Deployment WG Meeting
- Use-Case WG Meeting
- Domain-specific Model WG Mtg.
- Member Representative Committee Mtg.

**2027 Working Group Schedule Under Development**


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Upcoming WG Meetings

- December
  - NERC GADS Reporting LLM Implementation
    - Chevron & Turbine Logic
  - Working Group Deliverables: deep dive
    - Bijan Hosseininejad

- Starting in 2027
  - Alternating monthly meetings with the Energy Sector-specific Intelligence/Use-Cases WG
  - Working on aligning topics with a focus on lesson learned and tech transfer from AI implementation and scaling





© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Hardware Accelerated Security at the Edge (HASE)

## AI Isolation and Edge Based Analytics for Security

Jeremy Lawrence, PI Cyber Security for Generation Assets

November 11, 2026



© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Where Should Your AI Live?

Hardware-Accelerated Security at the Edge

1. In the cloud?
2. In your utility data center?
3. Near a plant, substation, or device?


© 2026 Electric Power Research Institute, Inc. All rights reserved.
13

# Cyber AI Has Three Jobs

Use AI for defense. Secure the AI. Prepare for attackers using AI.

01

## Protect With AI

Find threats and help analysts respond.

02

## Protect The AI

Secure models, data, hardware, and software.

03

## Protect From AI

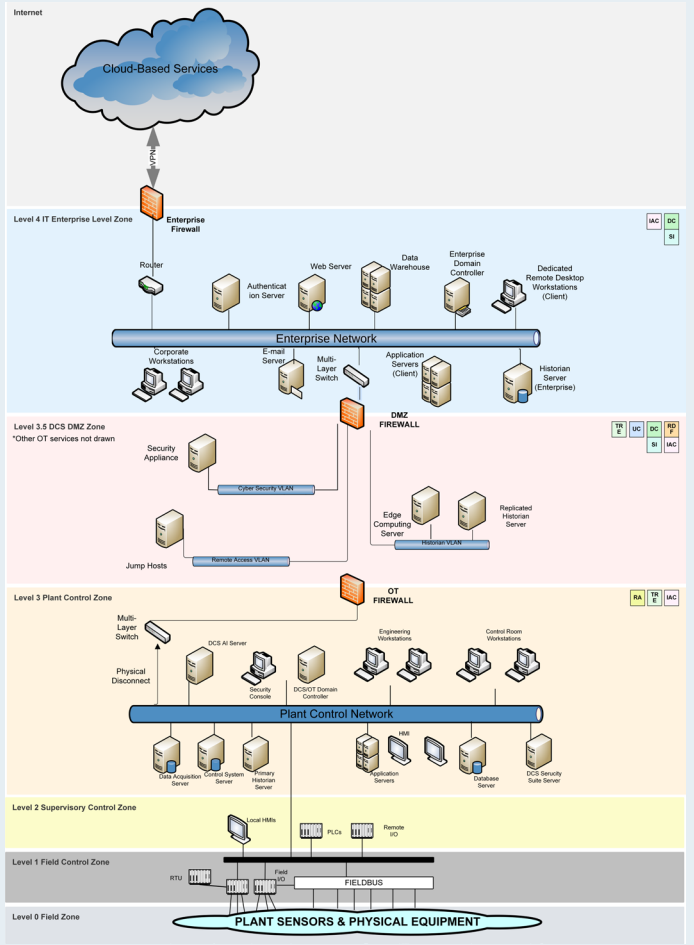
Prepare for faster, more adaptive attacks.


© 2026 Electric Power Research Institute, Inc. All rights reserved.
14

# Utility Systems Have Different Needs

Utility AI must work safely and reliably around physical equipment.

1. **Equipment must remain available**
2. **Mistakes can have physical effects**
3. **Internet access may be limited or restricted**
4. **Some utility equipment operates for decades**






© 2026 Electric Power Research Institute, Inc. All rights reserved.

15

# HASE Enables Security to the Edge

DOE-sponsored research tests security near utility equipment.

1. Designed for operational technology (OT) environments
2. Monitors activity close to utility assets
3. Combines local and central analysis
4. Must improve security without disrupting operations
5. Pre-compute module with pathway for local inference embedded in control systems

RESEARCH QUESTION

**What are the implications and feasibility to deploy AI-based security at the edge?**


© 2026 Electric Power Research Institute, Inc. All rights reserved.
16

# A DPU Gives Security Its Own Compute

A Data Processing Unit provides separate resources for security work.

1. **Replacement for Traditional Networking Cards**
   Has its own processor and memory
   Connects directly to network traffic

2. **Runs selected security work separately**
   Reduces dependence on the main computer

3. **Used in Data Centers for High Performance Networking**
   400Gbs+ Throughput



NVIDIA BlueField-3 Data Processing Unit


© 2026 Electric Power Research Institute, Inc. All rights reserved.
17

# Integrated Team Testbed

Different partners design, build, operate, challenge, and measure HASE.

1. **Security Researchers**
   guide and integrate the project

2. **Technology partners**
   provide hardware and develop software
   long term commercialization

3. **Test beds**
   provide realistic test environments

4. **Security red teams**
   simulate attacks and measure results

RESEARCH COLLABORATORS

EPRI

Clemson

University of North Carolina Charlotte

Emerson

Ameren

Southern Company

NVIDIA

waterfall

# Security Isolation Important

Attackers are known to disable security defenses

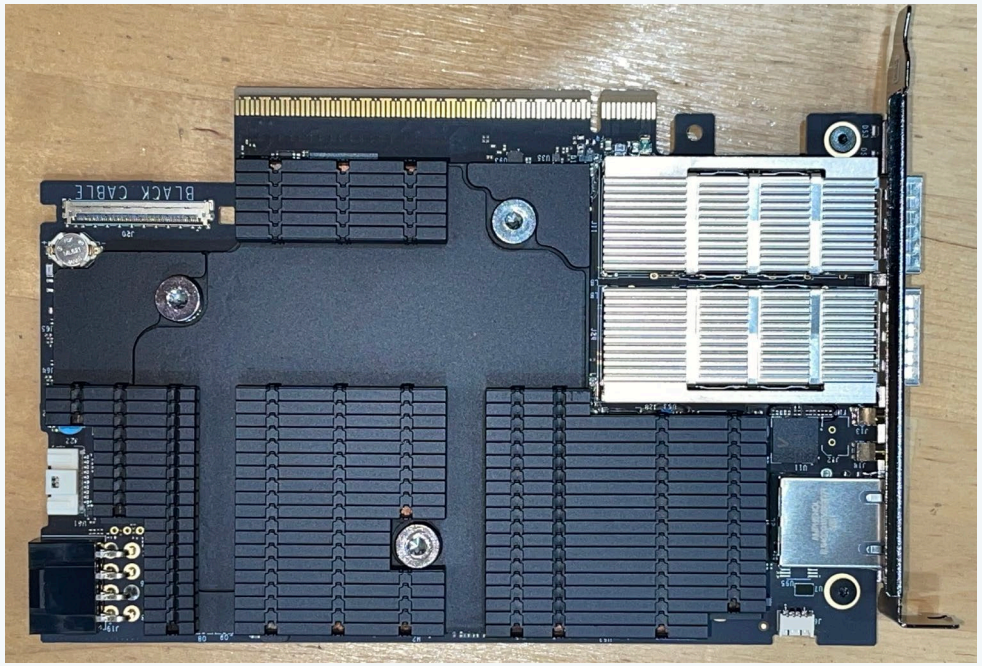
## Software agent

- Runs inside the main computer
- Shares the operating system
- Sees detailed host activity
- May be affected by a host attack

## DPU-based security

- Runs on separate hardware
- Uses dedicated resources
- Watches network activity independently
- Adds another security boundary







© 2026 Electric Power Research Institute, Inc. All rights reserved.

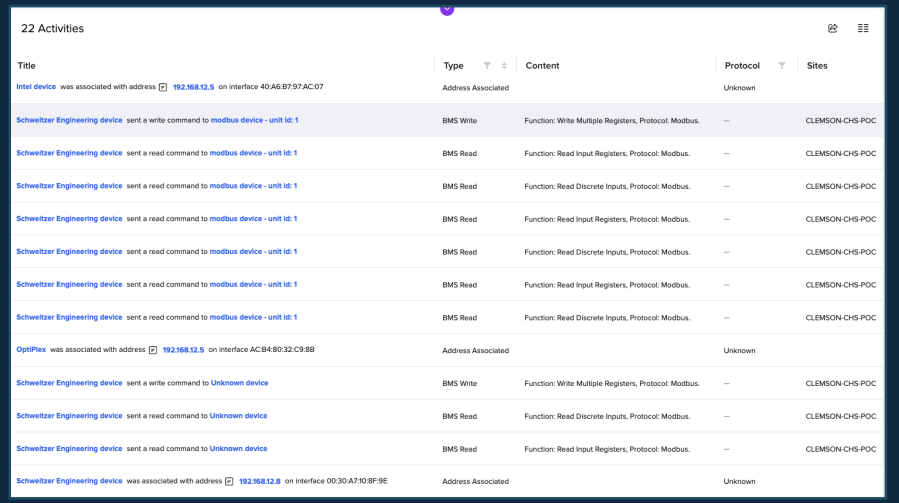
19

# Deployment in Practice

A separate DPU observes network activity and feeds centralized AI analytics.

1. DPU embedded in test server
2. Integrated into control system HMIs, application servers, and engineering workstations (virtual adapters)
3. DPU compute pre-processes network traffic and device characteristics (edge)
4. Centralized AI analytics to detect attacks
5. Local AI analytics for attack detection (future)

## DPU VIEW: INDEPENDENT NETWORK ACTIVITY LOG



22 Activities

| Title | Type | Content | Protocol | Sites |
|---|---|---|---|---|
| Intel device was associated with address 192.168.12.5 on interface 40:A6:B7:97:AC:07 | Address Associated | | Unknown | |
| Schweitzer Engineering device sent a write command to modbus device - unit id: 1 | BMS Write | Function: Write Multiple Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Input Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Discrete Inputs, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Input Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Discrete Inputs, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Input Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Discrete Inputs, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| OptiPlex was associated with address 192.168.12.5 on interface AC:B4:80:32:C9:8B | Address Associated | | Unknown | |
| Schweitzer Engineering device sent a write command to Unknown device | BMS Write | Function: Write Multiple Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to Unknown device | BMS Read | Function: Read Discrete Inputs, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to Unknown device | BMS Read | Function: Read Input Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device was associated with address 192.168.12.8 on interface 00:30:A7:10:8F:9E | Address Associated | | Unknown | |

Separate hardware observes device activity without relying on the host.


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# HASE Objectives

## Protect With AI

- Find unusual behavior
- Connect related warning signs
- Help analysts investigate faster
- **Today**: Frontier models to analyze alerts
- **Future State:** Move models embedded in the edge (lower Levels of OT)

## Protect the AI

- Separate security from the host
- Verify systems and software
- Protect data and settings
- Deterministic isolation technologies

# Establishing AI Guardrails for AI-Enabled Attack Scenarios

**Testing AI vs AI**

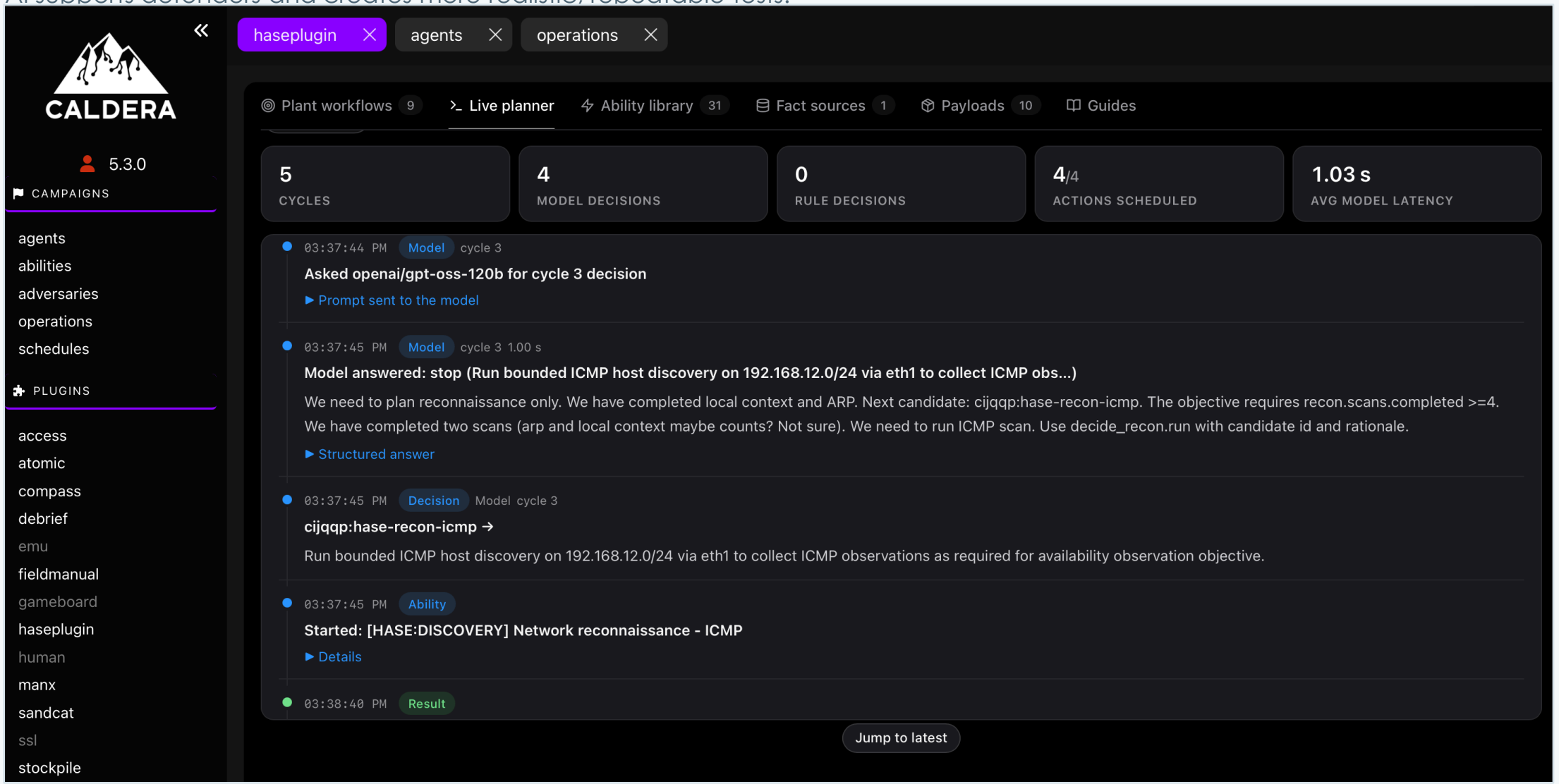
**Using a custom agentic planner to sequence attacks**

| AI Guardrail Category | Description | Applied Controls for HASE Testing |
|---|---|---|
| **Data Guardrails** | Controls on AI Inputs and outputs, so training data, retrieval sources, and prompts aren't poisoned and sensitive information doesn't leak. | Use only non-sensitive laboratory environment for testing. |
| **Model Guardrails** | Controls on the model itself so it behaves as intended even under cyber attacks. This also includes model weights and fine-tuning parameters that impact model performance. | Capture, log, and analyze inputs and outputs throughout testing. |
| **Application Guardrails** | Controls around how the software stack uses the model, so a manipulation or wrong model output can't impact the stack. | Limiting attack abilities to only those provided and deemed acceptable. Limit defined network range. Provided through containerized application. |
| **Infrastructure Guardrails** | Hardening the compute, orchestration, storage, and API's that host AI workloads, so the software stack is not exposed. | Dedicated kill switch, network restrictions on access, limitations on proxy server. |


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# AI Assisted Attacks

AI supports defenders and creates more realistic, repeatable tests.






© 2026 Electric Power Research Institute, Inc. All rights reserved.

23

# Model Appropriate for Attack

Currently testing multiple models in attack execution



1. **Rules**
   Deterministic. Handle known and repeatable checks.

2. **Traditional machine learning**
   Handles classification

3. **Small language models**
   Support focused local tasks

4. **Large and frontier models**
   Support broad or detailed reasoning


© 2026 Electric Power Research Institute, Inc. All rights reserved.
24

# Put Each Model Where It Works Best

Edge, data center, cloud, and people can share the work.



## Edge

Rules, machine learning, and small models



## Utility data center

Analysis across sites and systems



## Cloud

Frontier models when capability is justified



## People

Review evidence and approve important actions


© 2026 Electric Power Research Institute, Inc. All rights reserved.
25

# Summary

HASE tested to improve security without negative impacts to control system operations.

- Testing and Analysis in Progress
- Help analysts identify and respond faster
- Isolation Environment to Withstand Attacks
- Avoid unacceptable effects on performance or availability

## Questions


© 2026 Electric Power Research Institute, Inc. All rights reserved.
26

# Walz, Oral History Application

## Avery Hodges, EPRI


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Walz - Oral History App

## Knowledge Capture & Retention

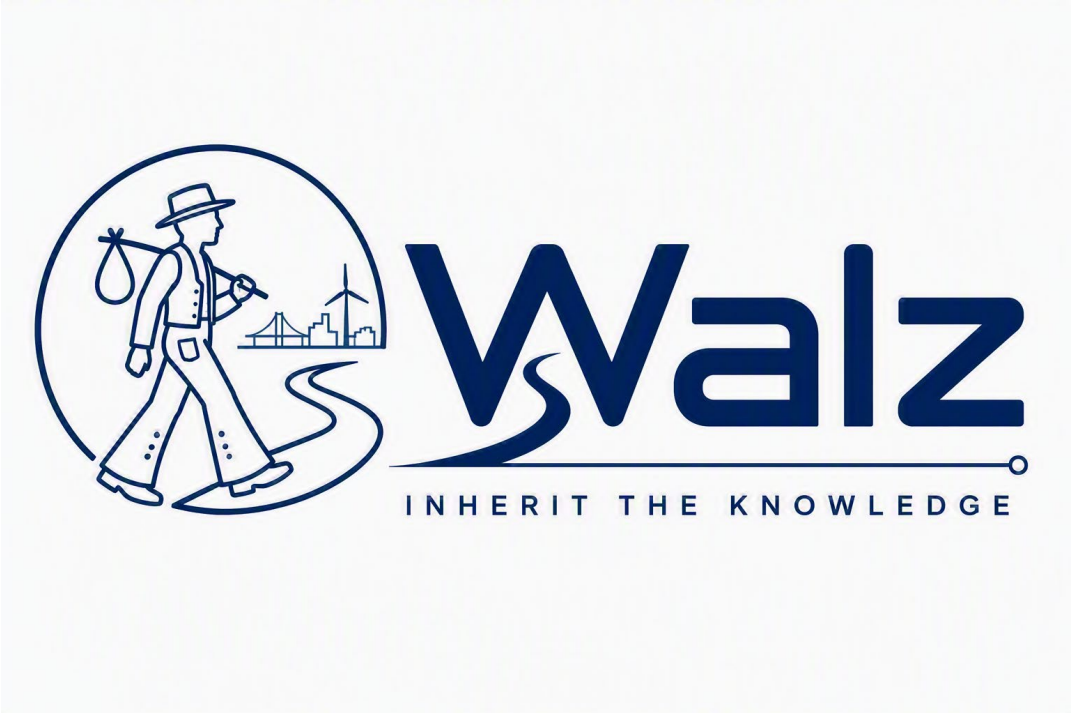
Dr. Lea Boche
lboche@epri.com

Avery Hodges
ahodges@epri.com



© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Why Capture Oral History?




**Problem: Subject Matter Experts (SMEs) hold hidden knowledge that is**

- Not written in reports
- Not recorded in webcasts
- Only shared verbally

**Solution: Create a formal process to**

- Capture SME knowledge efficiently
- Preserve expertise across generations
- Share lessons learned across the power industry


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Knowledge Capture & Retrieval Architecture

**1. Capture**

Oral histories are recorded and ingested into the app.

**2. Transcribe**

On-premises Whisper turns audio into accurate transcripts.

**3. Anonymize**

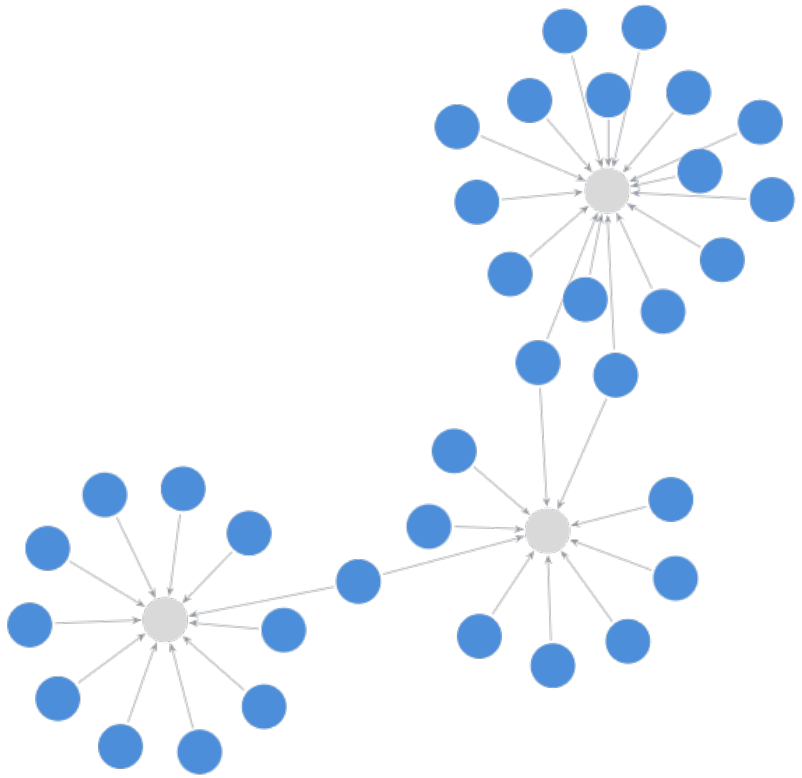
Sensitive details are stripped to protect privacy.

**4. Connect**

A knowledge graph links plant configuration, assets, and skills.

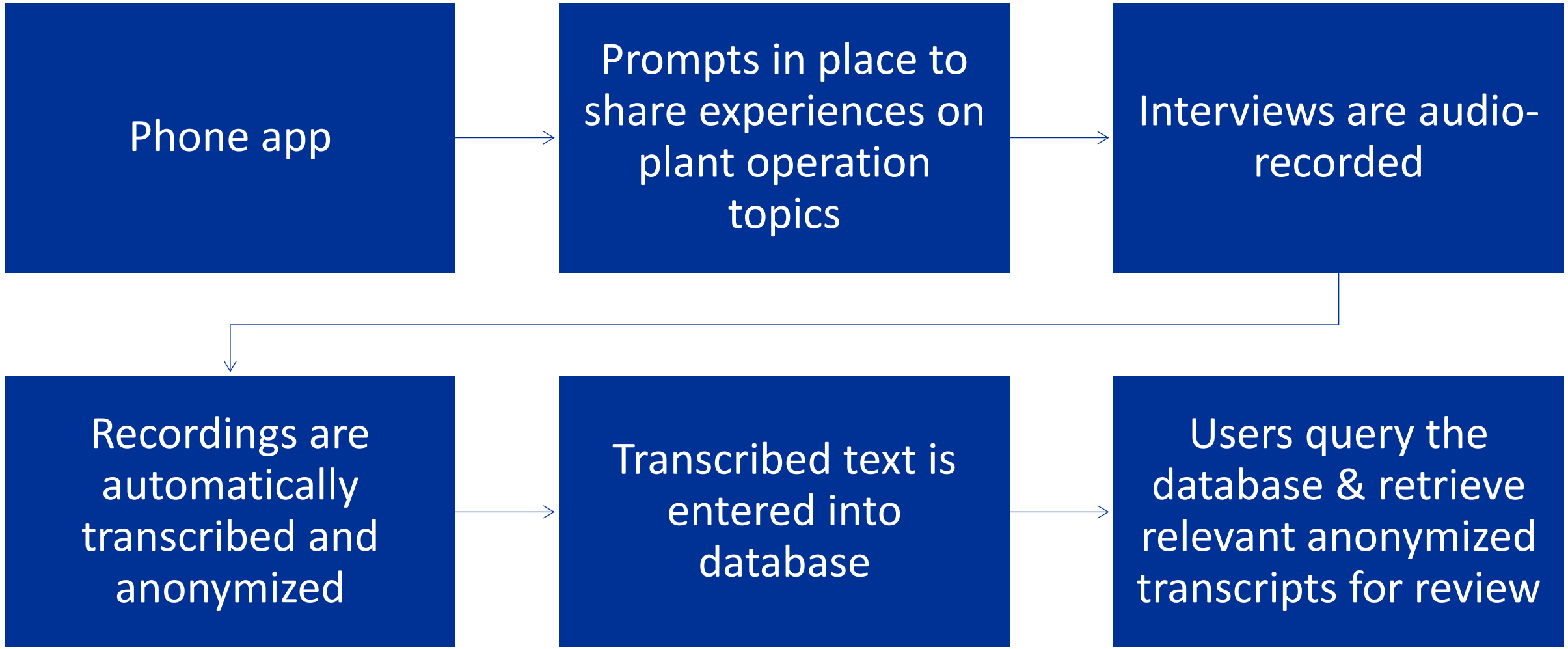
**5. Retrieve**

An LLM answers questions over the searchable archive.




© 2026 Electric Power Research Institute, Inc. All rights reserved.

# User Experience Pipeline




**Goal: Knowledge Retention, Storage, Searchability**


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Searching Through Knowledge: An Example

## User Query → App Searches → Retrieved Results

"Show me interviews that mentioned startup issues for feedwater pumps at nuclear plants."

- Asset:
  Feedwater Pump
- Incident:
  Startup Event
- Plant type:
  Nuclear
- Source:
  All Transcripts

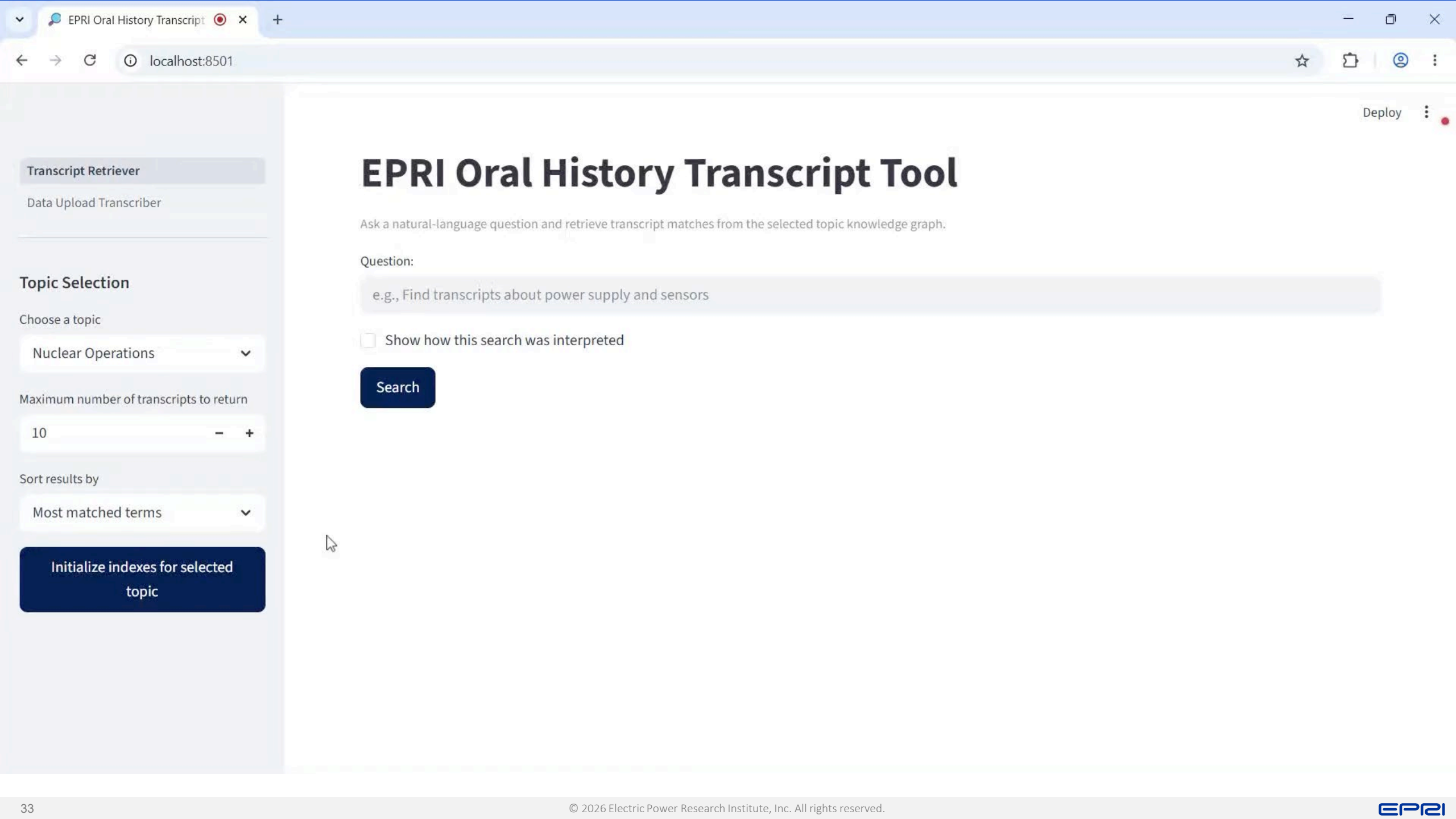
- Interview 011

"During startup, we noticed vibration at <LOCATION>, and …"

- Interview 148

"In a situation like this, <NAME> and I went to double-check valve…"

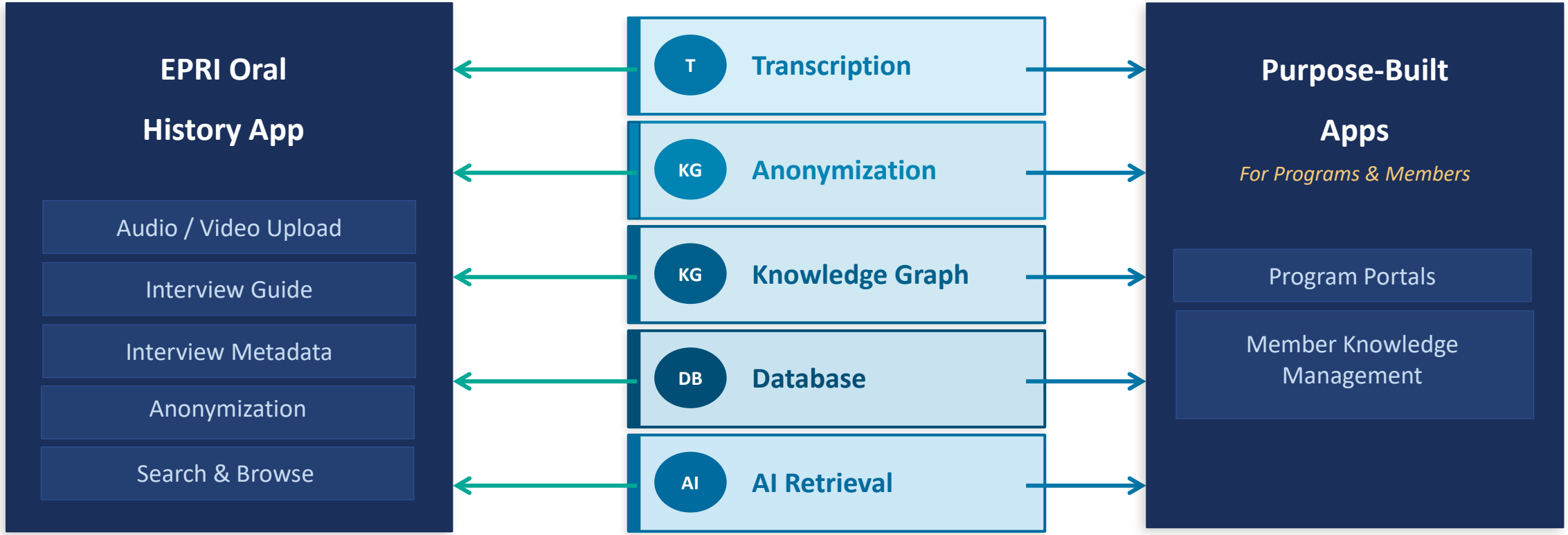

© 2026 Electric Power Research Institute, Inc. All rights reserved.





© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Vision for the Tool(s)





© 2026 Electric Power Research Institute, Inc. All rights reserved.

# WALZ

INHERIT THE KNOWLEDGE

## Secure Knowledge Capture and KAG-Powered Discovery

Guided interviews • Privacy-first processing • Structured evidence • EPRI-hosted

## 1 KNOWLEDGE CAPTURE & PROCESSING

Guided conversation to governed knowledge

**1 GUIDE**
**Dedicated interview guide**
Tiered prompts
Consistent knowledge capture

**2 CAPTURE**
**Interview audio**
SME experiences
Secure recording input

**3 TRANSCRIBE**
**Whisper**
On-premises speech-to-text
Transcript draft

**4 ANONYMIZE**
**Microsoft Presidio**
Custom utility-name list
Custom location list

**5 PROCESS**
**Python processing**
Timestamp boundaries
Token-window segments

**6 STORE + STRUCTURE**
**PostgreSQL + Neo4j**
Redacted transcript + metadata
Entities, relationships
Embeddings + vector index

INTERVIEW-GUIDED CAPTURE

REDACTED TEXT DOWNSTREAM

RELATIONSHIP-FIRST GRAPH

## 2 KNOWLEDGE DISCOVERY PIPELINE

KAG • KNOWLEDGE-AUGMENTED

**1 ASK**
**Natural-language query**
User searches WALZ

**2 UNDERSTAND**
**Gemma-3-27B**
Query intent
Query embedding

**3 RETRIEVE**
**Neo4j vector search**
Top matching chunks
Similarity + graph context

**4 RANK**
**Transcript aggregation**
Group by transcript ID
Rank matching interviews

**5 GROUND**
**KAG**
Graph relationships
Transcript evidence + metadata

**6 PRESENT**
**WALZ interface**
Relevant interviews
Matched excerpts + connections

SEMANTIC + GRAPH RETRIEVAL

GROUNDED IN REDACTED EVIDENCE

## DATA PLACEMENT & PLATFORM

- **OBJECT STORAGE**
  Encrypted interview audio
  Enterprise object storage
- **POSTGRESQL**
  Authoritative redacted text
  Versions, metadata, processing status
- **NEO4J**
  Entities, relationships, provenance
  Chunk embeddings + vector index
- **APPLICATION**
  Streamlit user interface
  Python / API services
- **LLM**
  Gemma-3-27B
  Keyword extraction + querying

**EPRI ENTERPRISE INFRASTRUCTURE**

- On-premises operation
- Internal data governance
- Privacy-first architecture
- No public-cloud dependency

# Supplemental Project Notice: Walz Portal

- **Deliverables**
  - Oral history app and web platform; transcription and anonymization workflow
  - Initial anonymized transcript database and hybrid search framework
  - Participant-specific knowledge graphs and interview guides
- **Price and Schedule**
  - $40,000 total; minimum of five funders required for full scope
  - Two-year project; first website rollout targeted for late 2027
- **Contacts**
  - Lea Boche, lboche@epri.com
  - Avery Hodges, ahodges@epri.com

## Objective

- Reduce the risk of knowledge loss from workforce transitions and retirements
- Pilot a mobile and web platform that captures expert insights and lessons learned not documented elsewhere

## Approach

- Guided interviews, transcription, and anonymization into a secure, searchable repository
- LLM-enabled summaries paired with rules-based search for traceable answers

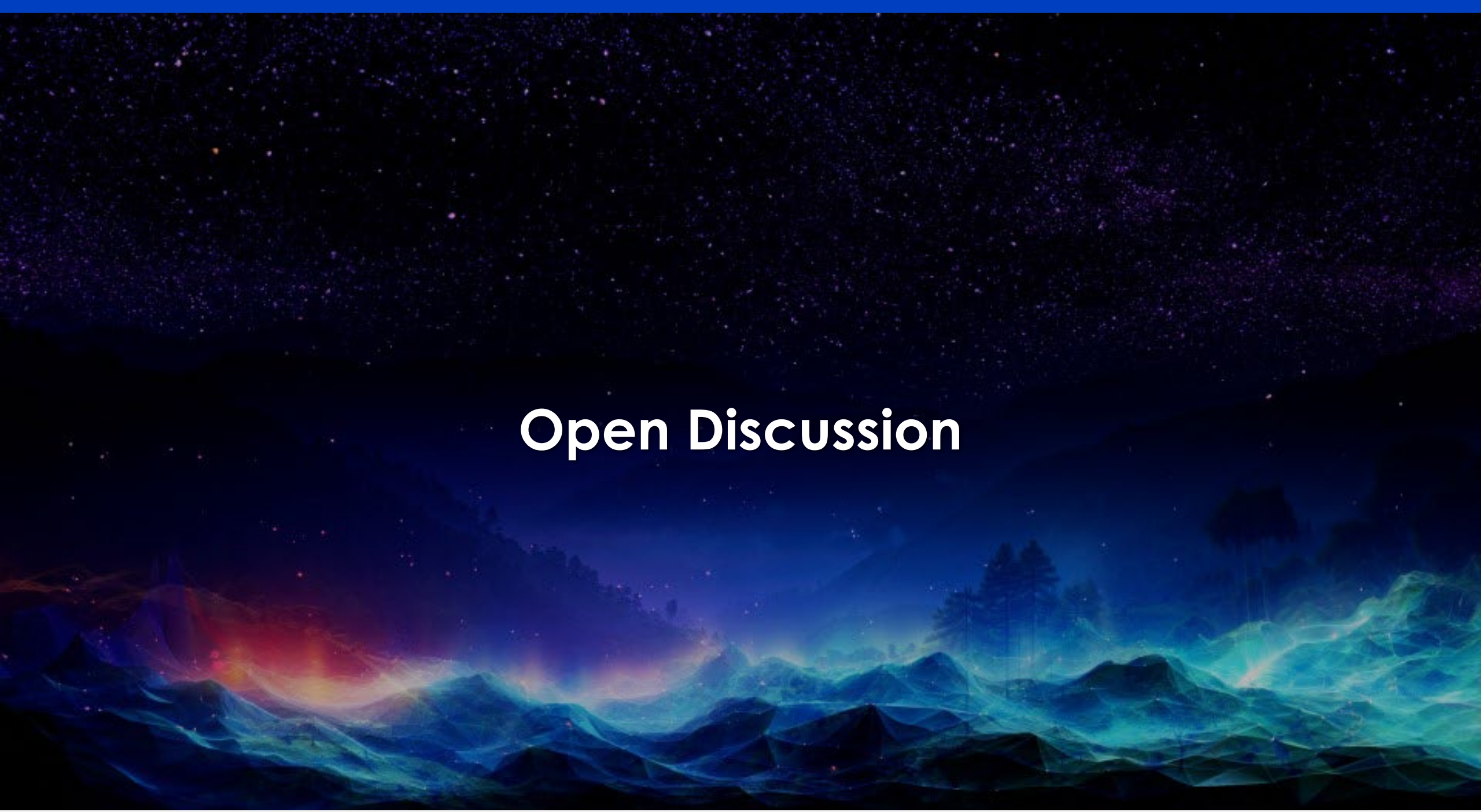
***https://www.epri.com/research/products/000000003002036852***


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# TOGETHER…SHAPING THE FUTURE OF ENERGY®

www.epri.com

© 2026 Electric Power Research Institute, Inc. All rights reserved.





© 2026 Electric Power Research Institute, Inc. All rights reserved.

# TOGETHER…SHAPING THE FUTURE OF ENERGY®



OPEN POWER AI CONSORTIUM

www.epri.com

© 2026 Electric Power Research Institute, Inc. All rights reserved.



© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Hardware Accelerated Security at the Edge (HASE)

## AI Isolation and Edge Based Analytics for Security

Jeremy Lawrence, PI Cyber Security for Generation Assets

November 11, 2026



© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Where Should Your AI Live?

Hardware-Accelerated Security at the Edge

1. In the cloud?
2. In your utility data center?
3. Near a plant, substation, or device?


© 2026 Electric Power Research Institute, Inc. All rights reserved.
2

# Cyber AI Has Three Jobs

Use AI for defense. Secure the AI. Prepare for attackers using AI.

01

## Protect With AI

Find threats and help analysts respond.

02

## Protect The AI

Secure models, data, hardware, and software.

03

## Protect From AI

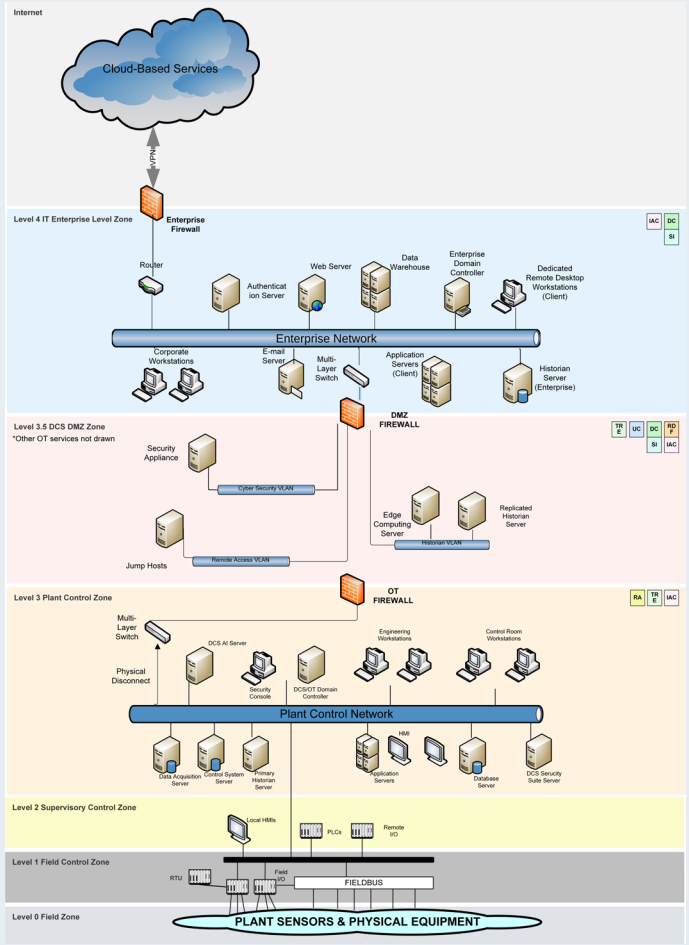
Prepare for faster, more adaptive attacks.


© 2026 Electric Power Research Institute, Inc. All rights reserved.
3

# Utility Systems Have Different Needs

Utility AI must work safely and reliably around physical equipment.

1. **Equipment must remain available**
2. **Mistakes can have physical effects**
3. **Internet access may be limited or restricted**
4. **Some utility equipment operates for decades**





© 2026 Electric Power Research Institute, Inc. All rights reserved.
4

# HASE Enables Security to the Edge

DOE-sponsored research tests security near utility equipment.

1. Designed for operational technology (OT) environments
2. Monitors activity close to utility assets
3. Combines local and central analysis
4. Must improve security without disrupting operations
5. Pre-compute module with pathway for local inference embedded in control systems

RESEARCH QUESTION

**What are the implications and feasibility to deploy AI-based security at the edge?**


© 2026 Electric Power Research Institute, Inc. All rights reserved.
5

# A DPU Gives Security Its Own Compute

A Data Processing Unit provides separate resources for security work.

1. **Replacement for Traditional Networking Cards**
   Has its own processor and memory
   Connects directly to network traffic

2. **Runs selected security work separately**
   Reduces dependence on the main computer

3. **Used in Data Centers for High Performance Networking**
   400Gbs+ Throughput



NVIDIA BlueField-3 Data Processing Unit


© 2026 Electric Power Research Institute, Inc. All rights reserved.
6

# Integrated Team Testbed

Different partners design, build, operate, challenge, and measure HASE.

1. **Security Researchers**
   guide and integrate the project

2. **Technology partners**
   provide hardware and develop software
   long term commercialization

3. **Test beds**
   provide realistic test environments

4. **Security red teams**
   simulate attacks and measure results

RESEARCH COLLABORATORS

EPRI
Clemson
University of North Carolina Charlotte
Emerson
Ameren
Southern Company
NVIDIA
waterfall

# Security Isolation Important

Attackers are known to disable security defenses

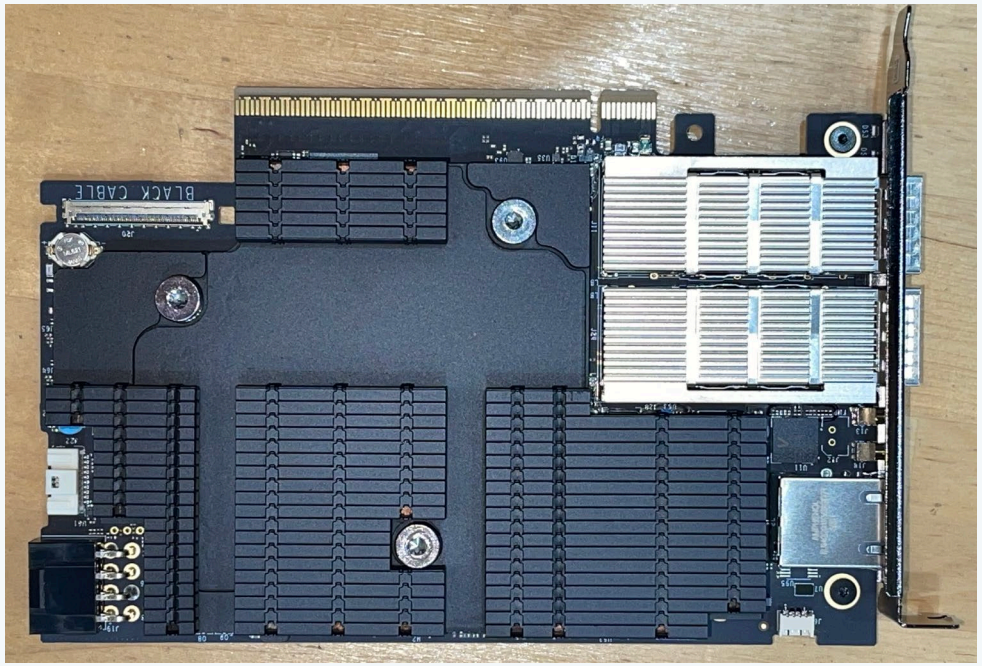
## Software agent

- Runs inside the main computer
- Shares the operating system
- Sees detailed host activity
- May be affected by a host attack



## DPU-based security

- Runs on separate hardware
- Uses dedicated resources
- Watches network activity independently
- Adds another security boundary





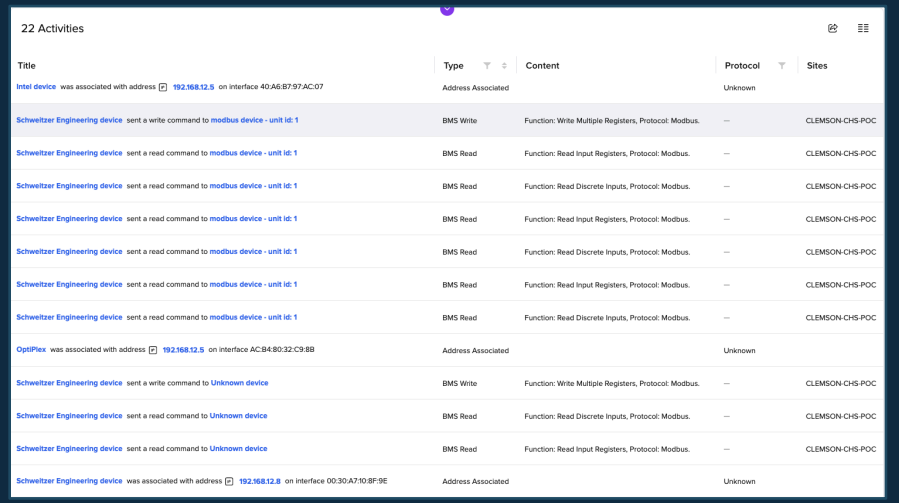
© 2026 Electric Power Research Institute, Inc. All rights reserved.
8

# Deployment in Practice

A separate DPU observes network activity and feeds centralized AI analytics.

1. DPU embedded in test server
2. Integrated into control system HMIs, application servers, and engineering workstations (virtual adapters)
3. DPU compute pre-processes network traffic and device characteristics (edge)
4. Centralized AI analytics to detect attacks
5. Local AI analytics for attack detection (future)

## DPU VIEW: INDEPENDENT NETWORK ACTIVITY LOG



22 Activities

| Title | Type | Content | Protocol | Sites |
|---|---|---|---|---|
| Intel device was associated with address 192.168.12.5 on interface 40:A6:B7:97:AC:07 | Address Associated | | Unknown | |
| Schweitzer Engineering device sent a write command to modbus device - unit id: 1 | BMS Write | Function: Write Multiple Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Input Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Discrete Inputs, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Input Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Discrete Inputs, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Input Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to modbus device - unit id: 1 | BMS Read | Function: Read Discrete Inputs, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| OptiPlex was associated with address 192.168.12.5 on interface AC:B4:80:32:C9:8B | Address Associated | | Unknown | |
| Schweitzer Engineering device sent a write command to Unknown device | BMS Write | Function: Write Multiple Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to Unknown device | BMS Read | Function: Read Discrete Inputs, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device sent a read command to Unknown device | BMS Read | Function: Read Input Registers, Protocol: Modbus. | – | CLEMSON-CHS-POC |
| Schweitzer Engineering device was associated with address 192.168.12.8 on interface 00:30:A7:10:8F:9E | Address Associated | | Unknown | |

Separate hardware observes device activity without relying on the host.


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# HASE Objectives

## Protect With AI

- Find unusual behavior
- Connect related warning signs
- Help analysts investigate faster
- **Today**: Frontier models to analyze alerts
- **Future State:** Move models embedded in the edge (lower Levels of OT)

## Protect the AI

- Separate security from the host
- Verify systems and software
- Protect data and settings
- Deterministic isolation technologies

# Establishing AI Guardrails for AI-Enabled Attack Scenarios

**Testing AI vs AI**

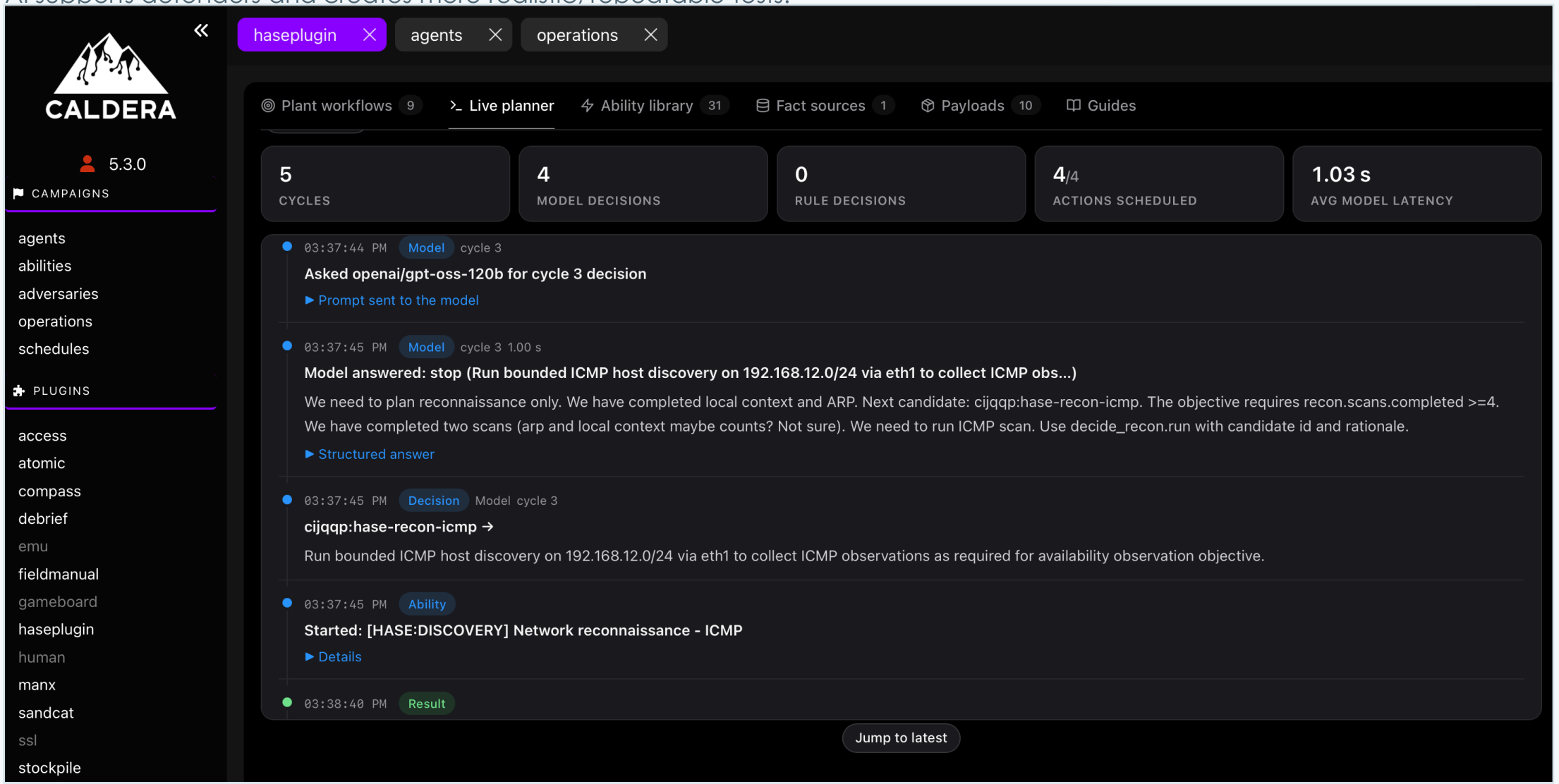
**Using a custom agentic planner to sequence attacks**

| AI Guardrail Category | Description | Applied Controls for HASE Testing |
|---|---|---|
| **Data Guardrails** | Controls on AI Inputs and outputs, so training data, retrieval sources, and prompts aren't poisoned and sensitive information doesn't leak. | Use only non-sensitive laboratory environment for testing. |
| **Model Guardrails** | Controls on the model itself so it behaves as intended even under cyber attacks. This also includes model weights and fine-tuning parameters that impact model performance. | Capture, log, and analyze inputs and outputs throughout testing. |
| **Application Guardrails** | Controls around how the software stack uses the model, so a manipulation or wrong model output can't impact the stack. | Limiting attack abilities to only those provided and deemed acceptable. Limit defined network range. Provided through containerized application. |
| **Infrastructure Guardrails** | Hardening the compute, orchestration, storage, and API's that host AI workloads, so the software stack is not exposed. | Dedicated kill switch, network restrictions on access, limitations on proxy server. |


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# AI Assisted Attacks

AI supports defenders and creates more realistic, repeatable tests.





© 2026 Electric Power Research Institute, Inc. All rights reserved.
12

# Model Appropriate for Attack

Currently testing multiple models in attack execution



1. **Rules**
   Deterministic. Handle known and repeatable checks.

2. **Traditional machine learning**
   Handles classification

3. **Small language models**
   Support focused local tasks

4. **Large and frontier models**
   Support broad or detailed reasoning


© 2026 Electric Power Research Institute, Inc. All rights reserved.
13

# Put Each Model Where It Works Best

Edge, data center, cloud, and people can share the work.



## Edge

Rules, machine learning, and small models



## Utility data center

Analysis across sites and systems



## Cloud

Frontier models when capability is justified



## People

Review evidence and approve important actions


© 2026 Electric Power Research Institute, Inc. All rights reserved.
14

# Summary

HASE tested to improve security without negative impacts to control system operations.



Testing and Analysis in Progress



Help analysts identify and respond faster



Isolation Environment to Withstand Attacks



Avoid unacceptable effects on performance or availability

## Questions



15

© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Walz - Oral History App

## Knowledge Capture & Retention

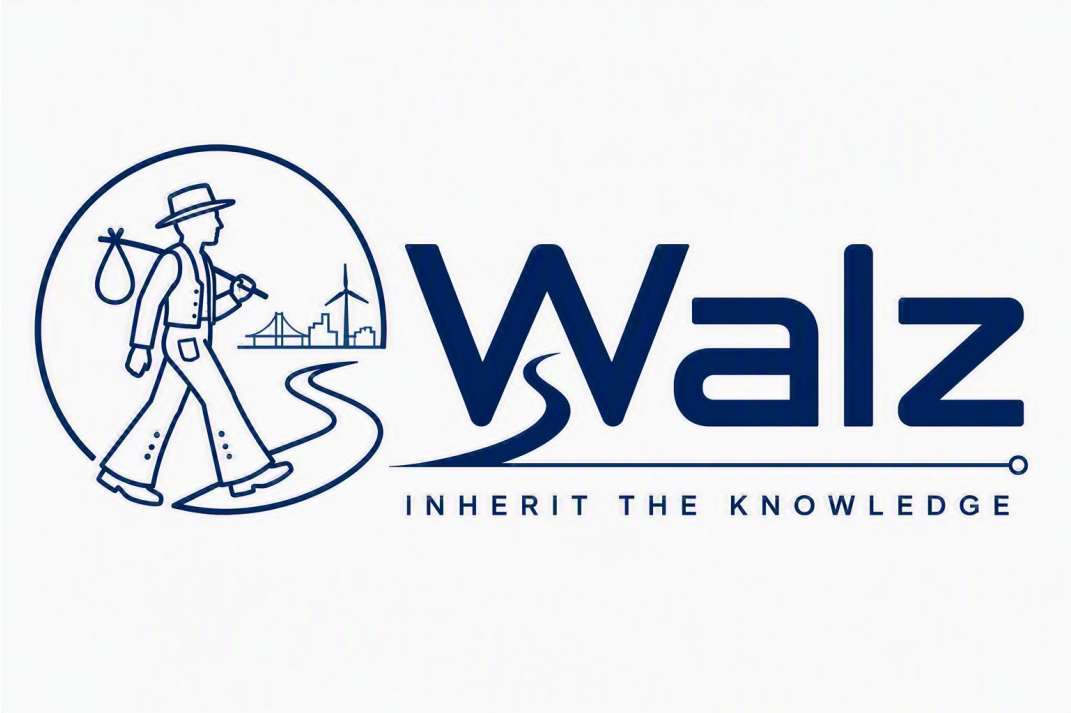
Dr. Lea Boche
lboche@epri.com

Avery Hodges
ahodges@epri.com



© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Why Capture Oral History?




**Problem: Subject Matter Experts (SMEs) hold hidden knowledge that is**

- Not written in reports
- Not recorded in webcasts
- Only shared verbally

**Solution: Create a formal process to**

- Capture SME knowledge efficiently
- Preserve expertise across generations
- Share lessons learned across the power industry


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Knowledge Capture & Retrieval Architecture

**1. Capture**

Oral histories are recorded and ingested into the app.

**2. Transcribe**

On-premises Whisper turns audio into accurate transcripts.

**3. Anonymize**

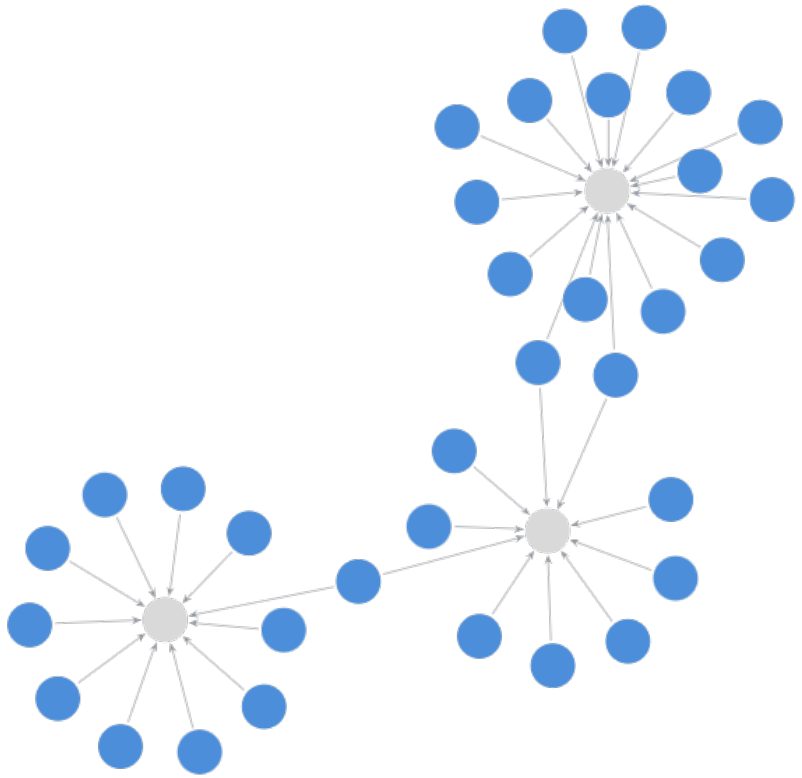
Sensitive details are stripped to protect privacy.

**4. Connect**

A knowledge graph links plant configuration, assets, and skills.

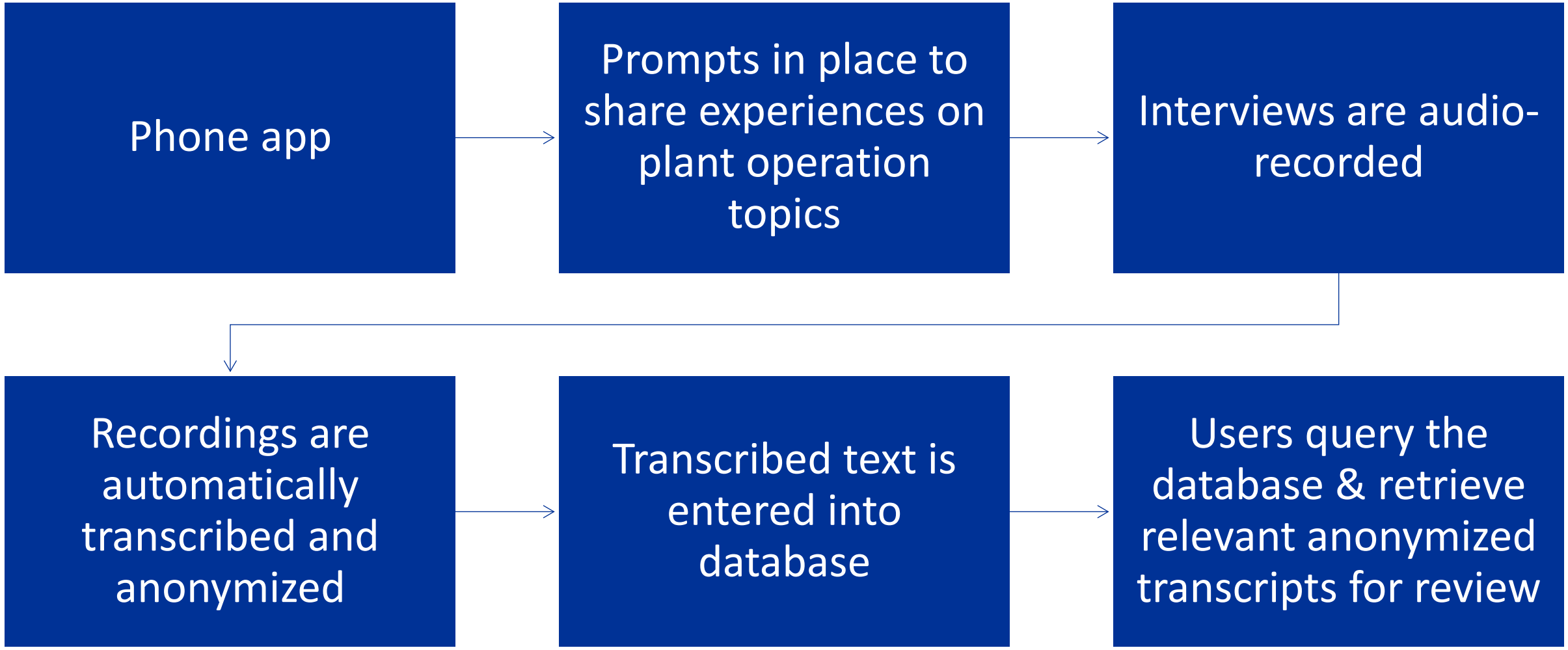
**5. Retrieve**

An LLM answers questions over the searchable archive.




© 2026 Electric Power Research Institute, Inc. All rights reserved.

# User Experience Pipeline




**Goal: Knowledge Retention, Storage, Searchability**


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Searching Through Knowledge: An Example

## User Query

"Show me interviews that mentioned startup issues for feedwater pumps at nuclear plants."

## App Searches

- Asset:
  Feedwater Pump
- Incident:
  Startup Event
- Plant type:
  Nuclear
- Source:
  All Transcripts

## Retrieved Results

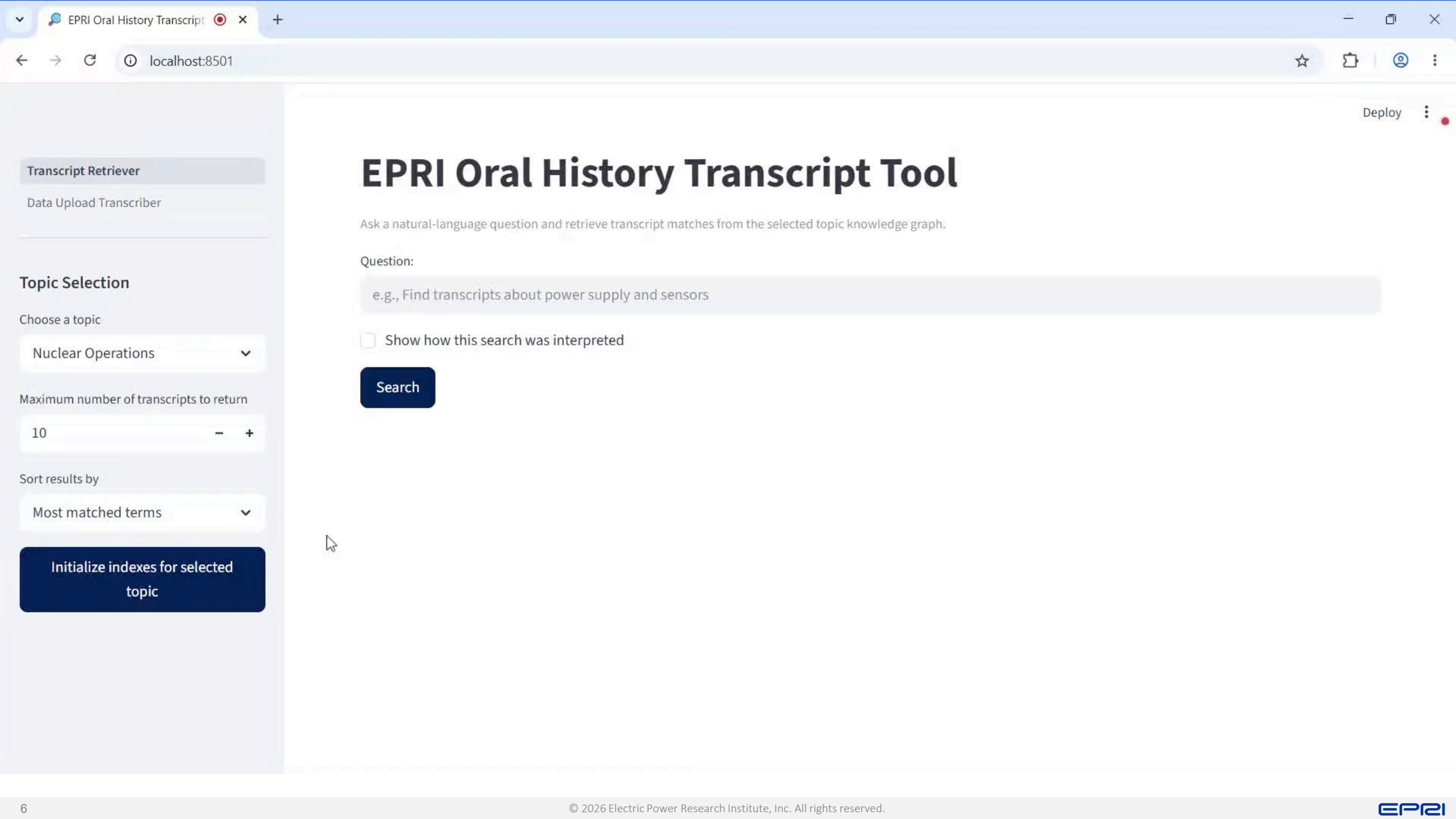
- Interview 011

"During startup, we noticed vibration at <LOCATION>, and …"

- Interview 148

"In a situation like this, <NAME> and I went to double-check valve…"

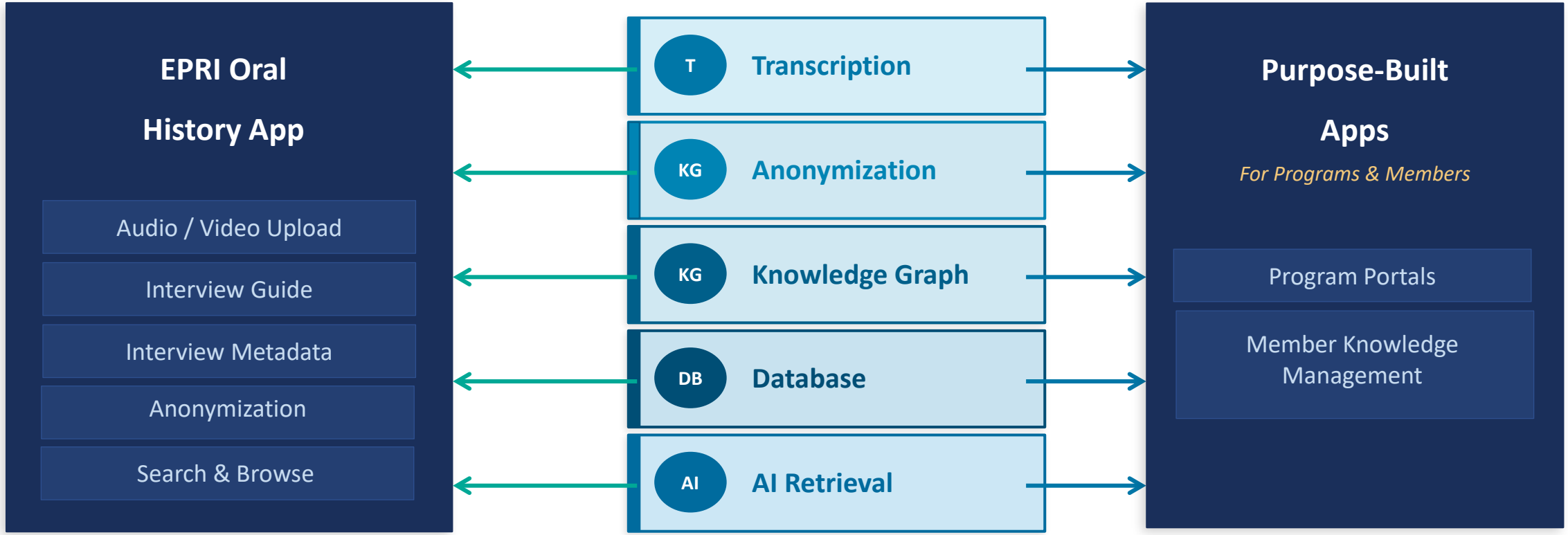

© 2026 Electric Power Research Institute, Inc. All rights reserved.





© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Vision for the Tool(s)





© 2026 Electric Power Research Institute, Inc. All rights reserved.

# WALZ

INHERIT THE KNOWLEDGE

## Secure Knowledge Capture and KAG-Powered Discovery

Guided interviews • Privacy-first processing • Structured evidence • EPRI-hosted

## 1 KNOWLEDGE CAPTURE & PROCESSING

Guided conversation to governed knowledge

**1 GUIDE**
**Dedicated interview guide**
Tiered prompts
Consistent knowledge capture

**2 CAPTURE**
**Interview audio**
SME experiences
Secure recording input

**3 TRANSCRIBE**
**Whisper**
On-premises speech-to-text
Transcript draft

**4 ANONYMIZE**
**Microsoft Presidio**
Custom utility-name list
Custom location list

**5 PROCESS**
**Python processing**
Timestamp boundaries
Token-window segments

**6 STORE + STRUCTURE**
**PostgreSQL + Neo4j**
Redacted transcript + metadata
Entities, relationships
Embeddings + vector index

INTERVIEW-GUIDED CAPTURE

REDACTED TEXT DOWNSTREAM

RELATIONSHIP-FIRST GRAPH

## 2 KNOWLEDGE DISCOVERY PIPELINE

KAG • KNOWLEDGE-AUGMENTED

**1 ASK**
**Natural-language query**
User searches WALZ

**2 UNDERSTAND**
**Gemma-3-27B**
Query intent
Query embedding

**3 RETRIEVE**
**Neo4j vector search**
Top matching chunks
Similarity + graph context

**4 RANK**
**Transcript aggregation**
Group by transcript ID
Rank matching interviews

**5 GROUND**
**KAG**
Graph relationships
Transcript evidence + metadata

**6 PRESENT**
**WALZ interface**
Relevant interviews
Matched excerpts + connections

SEMANTIC + GRAPH RETRIEVAL

GROUNDED IN REDACTED EVIDENCE

## DATA PLACEMENT & PLATFORM

- **OBJECT STORAGE**
  Encrypted interview audio
  Enterprise object storage
- **POSTGRESQL**
  Authoritative redacted text
  Versions, metadata, processing status
- **NEO4J**
  Entities, relationships, provenance
  Chunk embeddings + vector index
- **APPLICATION**
  Streamlit user interface
  Python / API services
- **LLM**
  Gemma-3-27B
  Keyword extraction + querying

**EPRI ENTERPRISE INFRASTRUCTURE**

- On-premises operation
- Internal data governance
- Privacy-first architecture
- No public-cloud dependency

# Supplemental Project Notice: Walz Portal

- **Deliverables**
  - Oral history app and web platform; transcription and anonymization workflow
  - Initial anonymized transcript database and hybrid search framework
  - Participant-specific knowledge graphs and interview guides
- **Price and Schedule**
  - $40,000 total; minimum of five funders required for full scope
  - Two-year project; first website rollout targeted for late 2027
- **Contacts**
  - Lea Boche, lboche@epri.com
  - Avery Hodges, ahodges@epri.com

## Objective

- Reduce the risk of knowledge loss from workforce transitions and retirements
- Pilot a mobile and web platform that captures expert insights and lessons learned not documented elsewhere

## Approach

- Guided interviews, transcription, and anonymization into a secure, searchable repository
- LLM-enabled summaries paired with rules-based search for traceable answers

***https://www.epri.com/research/products/000000003002036852***


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# TOGETHER…SHAPING THE FUTURE OF ENERGY®

www.epri.com

© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Ongoing Progress



Report on First Results



Internal Development & Testing of the app



Integration of Feedback



First Member Beta Test


© 2026 Electric Power Research Institute, Inc. All rights reserved.

# Core Objectives

| | |
|---|---|
| Capturing Undocumented Expertise | The app records informal knowledge and experiences to fill gaps in institutional memory effectively. |
| Supporting Knowledge Retention | A robust research database stores valuable insights, enhancing operational practices and fostering innovation. |
| Enabling Industry-wide Sharing | The app offers a scalable framework for sharing lessons and legacy information across the energy sector. |
| Ensuring Privacy and Security | Anonymization and secure data handling ensure compliance with privacy standards and maintain data integrity. |


© 2026 Electric Power Research Institute, Inc. All rights reserved.