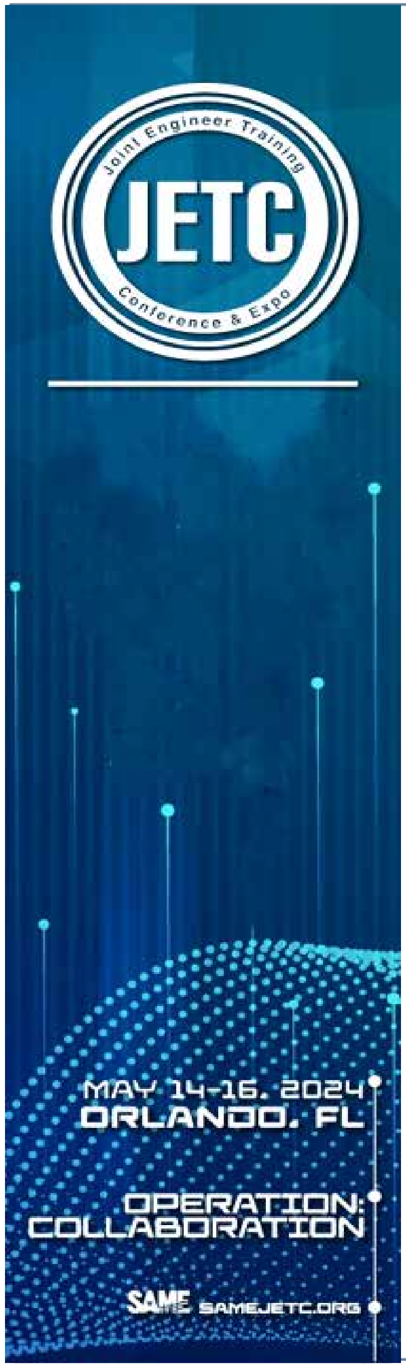
Cyber Resilience in AI-Driven Industrial Control Systems: Strategies and Innovations

Moderator: Mark R. Himes, Federal Market Leader, Olsson Inc.

Speakers:

- Jeremy Lawrence, Cyber Security Program Manager, EPRI
- Jason Hollern, Cyber Security Technical Executive, EPRI

May 15, 2024, 10:30 a.m.



This is an interactive session.
To participate, use your mobile device:
jetc.cnf.io
Or scan the QR Code

- Find the session.
- The presenter will unlock the poll(s) during the presentation.
- Please complete a brief Evaluation Survey at the end of the session.

HOUSEKEEPING ITEMS

- Take Note of Exits
- Silence Your Mobile Devices
- Presentations and Audio Recordings will be available in the Attendee Service Center until August 30, 2024
- Download your PDH record in the Attendee Service Center before August 30, 2024

Joint Engineer Training
JETC
Conference & Expo

MAY 14-16, 2024
ORLANDO, FL

OPERATION:
COLLABORATION

SAME SAMEJETC.ORG

MODERATOR

Mark R. Himes, PE

Olsson, Inc.

Federal Market Leader

Fun Facts

- Virginia Tech Hokies VT
- Hobbies: Golfing, Outdoors
- Did you Know I…played volleyball internationally

Joint Engineer Training
JETC
Conference & Expo

MAY 14-16, 2024
ORLANDO, FL

OPERATION: COLLABORATION

SAME SAMEJETC.ORG

SPEAKER

Jeremy Lawrence

Electric Power Research Institute

Cyber Security Program Manager

Fun Facts

- Former USN Submariner, CPO
- Hobbies: Water sports, boating, fishing, beach
- Kids sports Uber driver.

Joint Engineer Training
JETC
Conference & Expo

MAY 14-16, 2024
ORLANDO, FL

OPERATION:
COLLABORATION

SAME SAMEJETC.ORG

SPEAKER

Jason M. Hollern

Electric Power Research Institute
Technical Executive

Fun Facts

- The Ohio State Univ. Buckeyes
- Hobbies: Brewing, Single Board Computers (RPI)
- Did you Know I… published a cookbook.

Learning Objectives

Objective 1	Have a generalized understanding of how AI is being integrated into OT and other applications within the energy sector.
Objective 2	Grasp the concepts of how cyber attackers both target and use AI.
Objective 3	Make the linkage between IT and OT cyber security program implementation and operations as IT/OT convergence matures in the energy sector.
Objective 4	Connect best practice approaches for OT data security that can be applied to AI data sets and models.

EPRI

ADVANCING SAFE, RELIABLE, AFFORDABLE, AND CLEAN ENERGY FOR SOCIETY THROUGH GLOBAL COLLABORATION, SCIENCE AND TECHNOLOGY INNOVATION, AND APPLIED RESEARCH.

Together…Shaping the Future of Energy

The Landscape

Rapid Rise of Deep Fakes

Social Engineering: Attackers create a false sense of urgency to provide information, imitate a trusted person, pose as a position of authority.

- 74%: Involve Human Element (Error, Privilege Misuse, Stolen Credentials, Social Engineering)*

- 17% Of All Breaches involved Social Engineering (Top 3)*

*** 2023 Verizon DBIR**

Evolution of the Generation Landscape and Impacts

79%

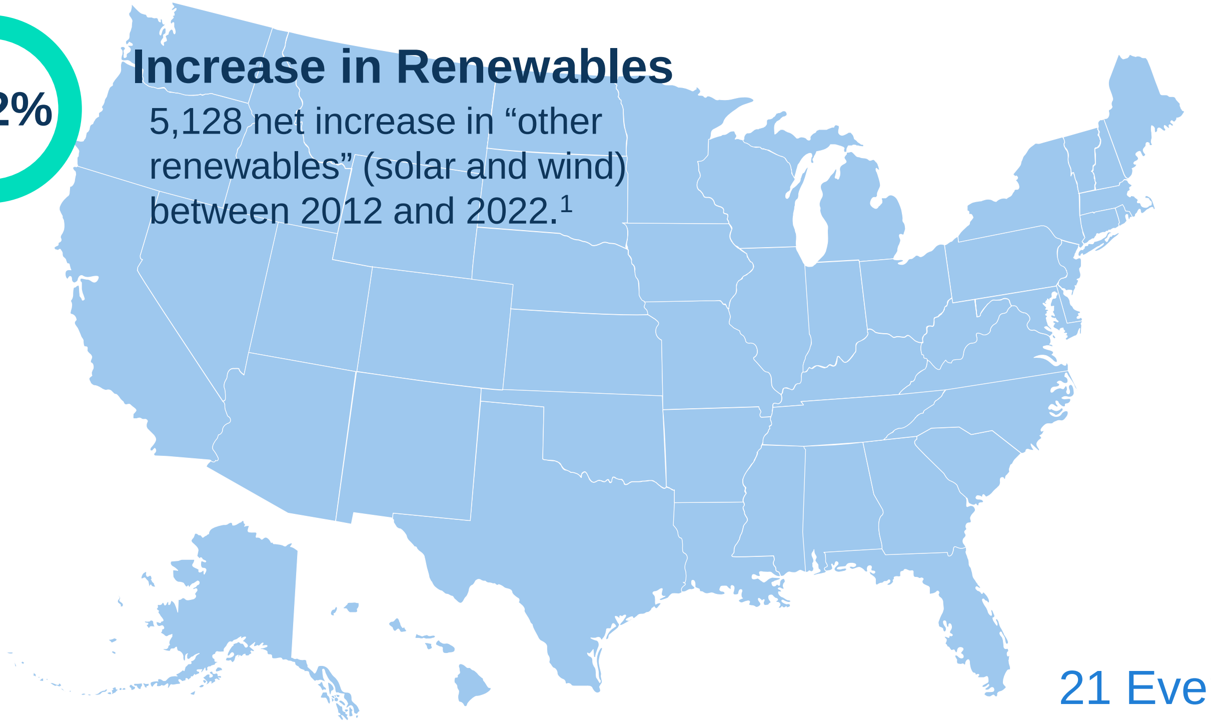
Increase in Facilities

5,541 net increase in power generation facilities between 2012 and 2022.[1]

262%

Increase in Renewables

5,128 net increase in “other renewables” (solar and wind) between 2012 and 2022.[1]



Attack Surface Larger attack surface, with more remotely monitored and operated facilities.

Physical Posture Less physical security presence.

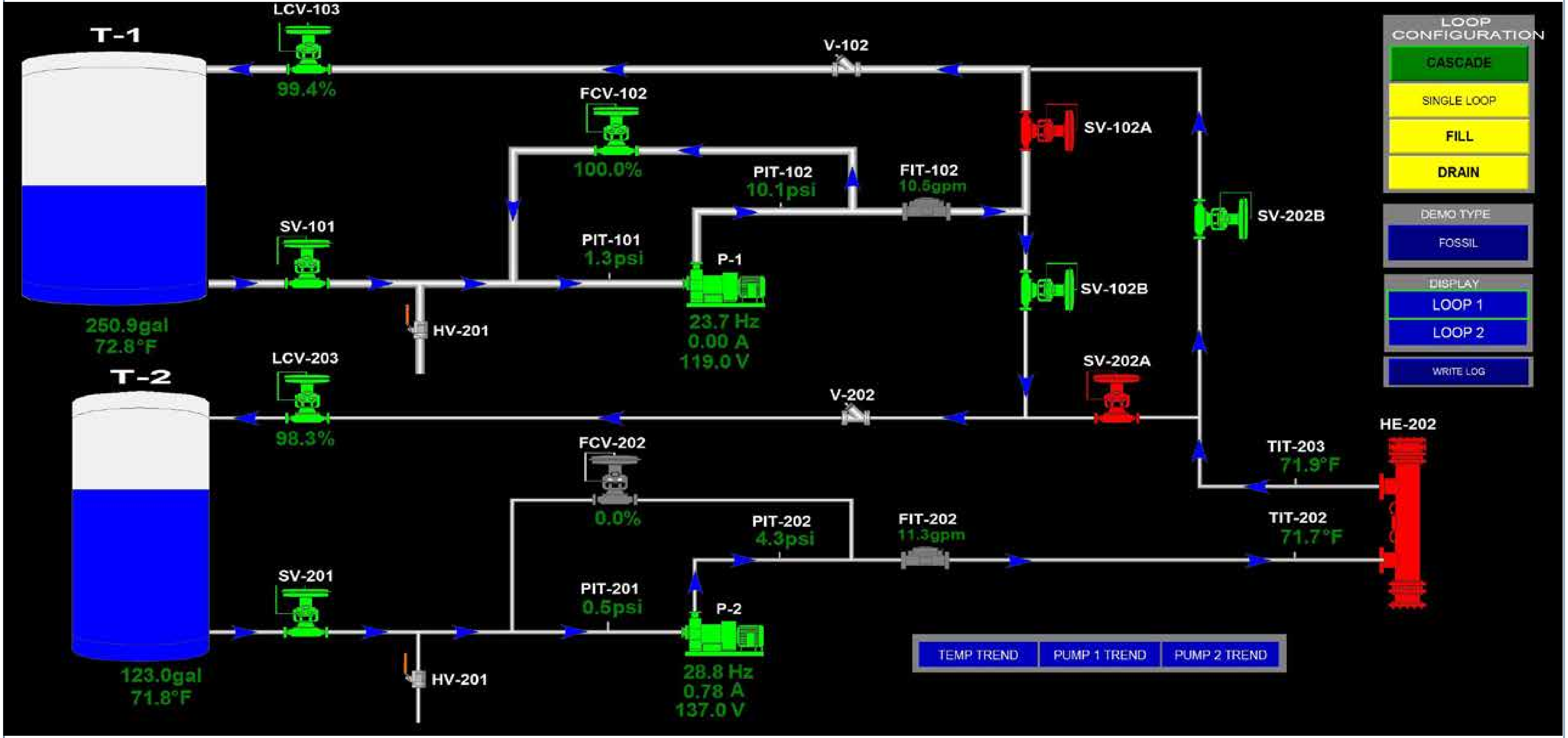
Distributed Larger distributed footprint.

US Statistics (as Reported DOE-417)
21 Events Reported Affecting Power Facilities 2021-2023

[1] https://www.eia.gov/electricity/annual/html/epa_04_01.html

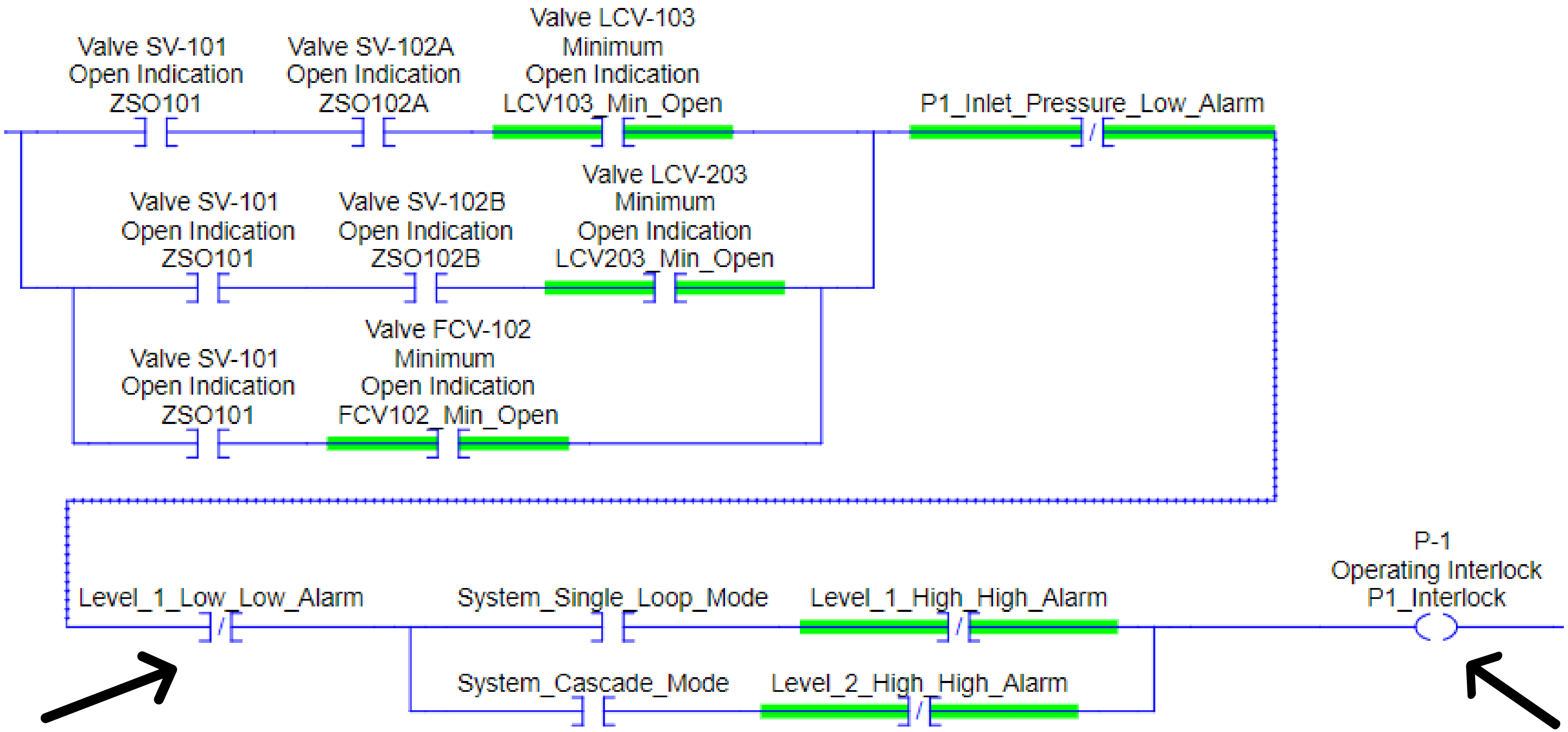
Live Content Slide

Poll: Dwell Time: Measures the time attackers have free access to a system. Considers the time to detect (MTTD) and respond (MTTR). What is the average Dwell Time for Attacks?


T-1
LCV-103
99.4%
V-102
FCV-102
100.0%
SV-102A
PIT-102
10.1psi
FIT-102
10.5gpm
SV-101
PIT-101
1.3psi
P-1
SV-202B
SV-102B
250.9gal
72.8°F
HV-201
23.7 Hz
0.00 A
119.0 V
T-2
LCV-203
98.3%
V-202
SV-202A
HE-202
TIT-203
71.9°F
FCV-202
0.0%
PIT-202
4.3psi
FIT-202
11.3gpm
TIT-202
71.7°F
SV-201
PIT-201
0.5psi
P-2
123.0gal
71.8°F
HV-201
28.8 Hz
0.78 A
137.0 V
LOOP CONFIGURATION
CASCADE
SINGLE LOOP
FILL
DRAIN
DEMO TYPE
FOSSIL
DISPLAY
LOOP 1
LOOP 2
WRITE LOG
TEMP TREND
PUMP 1 TREND
PUMP 2 TREND

P-1 Operating Interlock is TRUE if all conditions are met:

1. A viable flow path (combination of open valves)
2. Adequate inlet pressure (inlet pressure low alarm is FALSE)
3. Sufficiently high level in Tank 1, the pump's source (low low level alarm is FALSE)
4. Sufficiently low level in Tank where Pump P-1 is pumping into (corresponding tank high high level alarm is FALSE)



Live Content Slide

Poll: Think like an attacker: How can an attacker disrupt the system?

AI Security – Is it Really Different?

AI Changes the Game

Ladder Logic vs AI

Use cases for AI in OT.

Does a LLM always give the same result?

Increased Data Needs

Data, data, data…

Retraining models – different data flows

Attackers Targeting LLM’s

LLM01: Prompt Injection

LLM02: Insecure Output Handling

LLM03: Training Data Poisoning

LLM04: Model Denial of Service

LLM05: Supply Chain Vulnerabilities

LLM06: Sensitive Information Disclosure

LLM07: Insecure Plugin Design

LLM08: Excessive Agency

LLM09: Overreliance

LLM10: Model Theft

https://owasp.org/www-project-top-10-for-large-language-model-applications/

AI Cybersecurity Trinity

01

Protect AI

Models and data sets used for critical application

02

AI Security Tools

AI to help cyber teams in the trenches

03

AI Threat Landscape

Hackers can use AI too

What we are seeing in industry

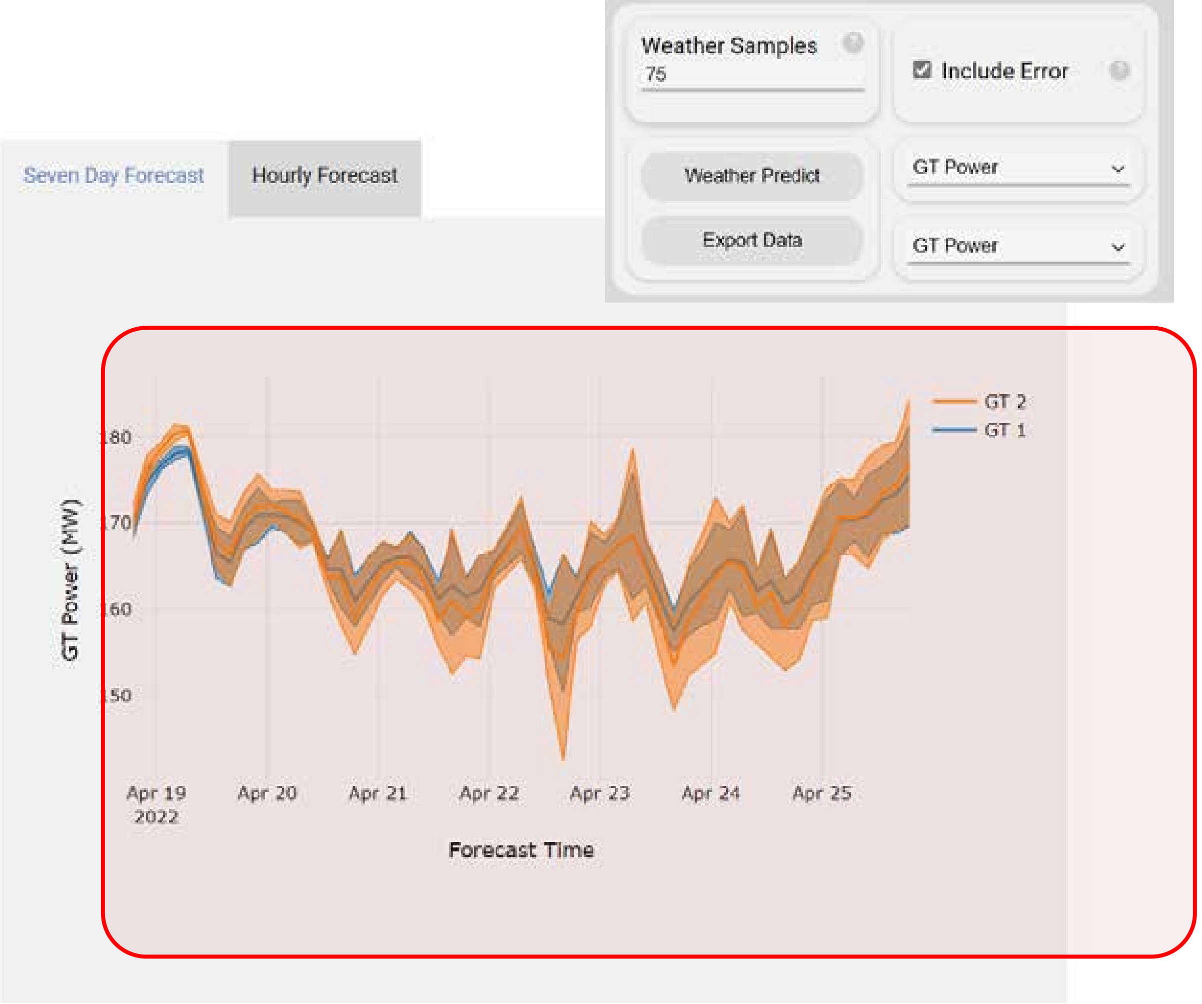
Protecting AI (Pillar 1) – Use Cases in Industry

- Power Generation Uses in AI Today
  - Operator/Engineer Aid
  - Control – ADEX
  - Anomaly Detection

OPTORA – Multi-Unit Dispatch Optimization

- Using digital twins of the assets, calibrated to actual site:
  - Weather conditions
  - Maintenance
  - Performance

- Using predictive analytics to determine which units to dispatch at which time to meet the load demand.



Weather Samples 75

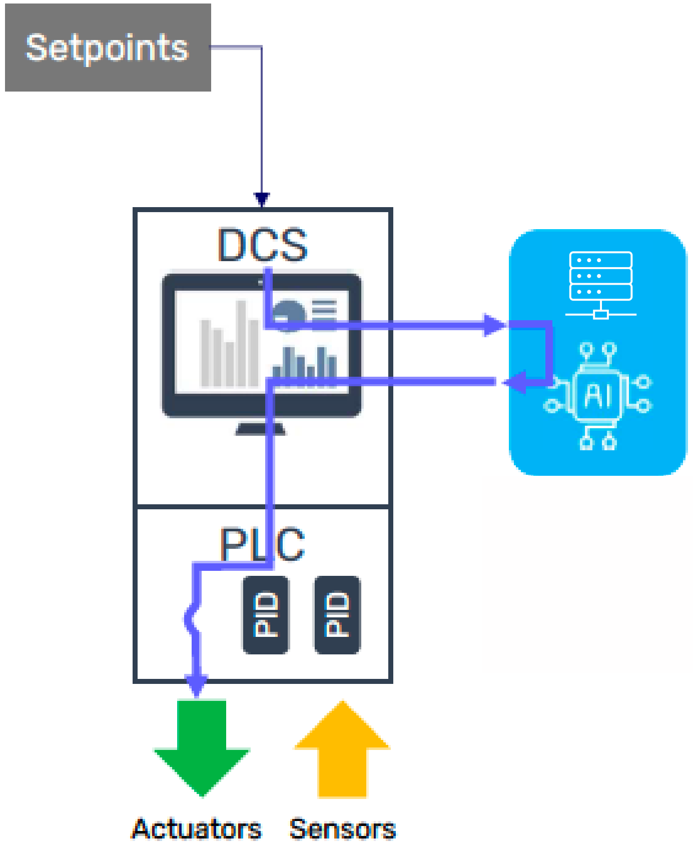
☑ Include Error

GT Power

GT Power

Real-Time Controls Autotuning

- Historian, sensor, and performance data is analyzed.
- AI algorithms use real-time plant data to understand plant conditions and what changes can be made to improve processes.
- AI algorithm changes DCS setpoints in real-time to optimize equipment performance.



Generative AI Use-Cases in Energy Sector

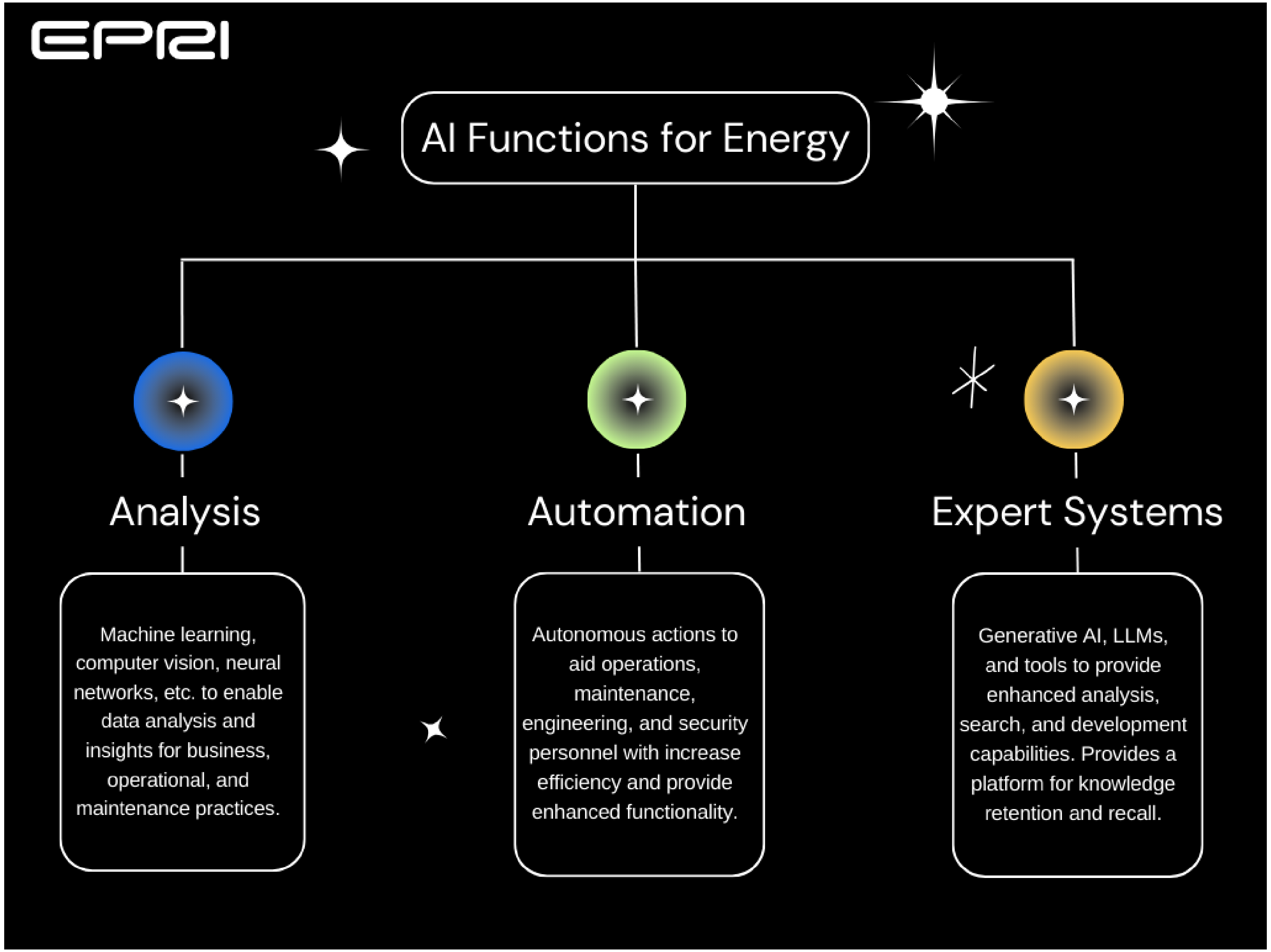
Internal Company Use-Case	Externally Facing Use-Case
Operational awareness	Level 1 customer assistance
Maintenance strategy analysis	Outage information generation
Regulatory analysis	Public communications, social media
Engineering resource support	Advanced usage/billing insights and reporting
Image generation to support CNN	Hiring, interviewing, human resources
Vegetation management analysis	Templates, websites, presentation designs
Process, procedure development	Tailored energy efficiency guidance

Security through AI – Advancements in Security

AI is already here for Energy

The future of AI will see implementation of tools and capability in OT systems and applications.

The power of AI comes when these functions can be integrated through various tools and applications to provide a force multiplier.



EPRI

AI Functions for Energy

Analysis

Machine learning, computer vision, neural networks, etc. to enable data analysis and insights for business, operational, and maintenance practices.

Automation

Autonomous actions to aid operations, maintenance, engineering, and security personnel with increase efficiency and provide enhanced functionality.

Expert Systems

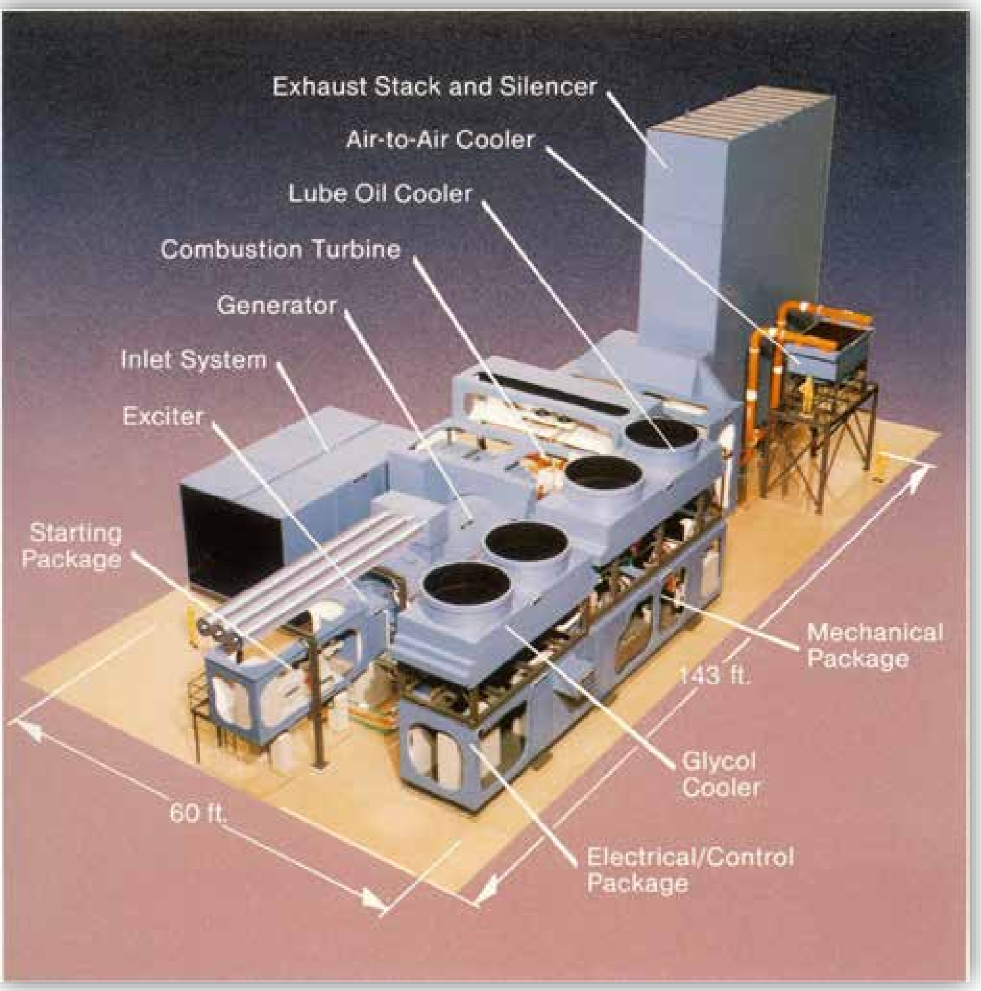
Generative AI, LLMs, and tools to provide enhanced analysis, search, and development capabilities. Provides a platform for knowledge retention and recall.

Live Content Slide

Poll: What is a digital twin?

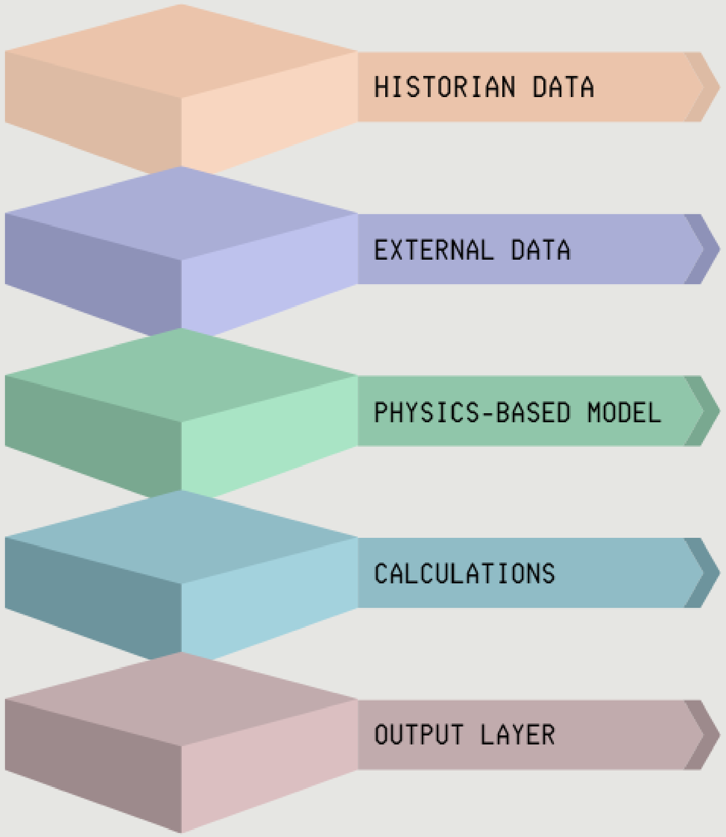
AI Driven Cyber Security

- Digital Twins for Anomaly Detection
  - Types of Digital Twins
  - Digital Twin vs. Actual Asset
  - Baselining, Testing, and Detection
  - Protecting the Digital Twin



Digital Twin Development

Hybrid Digital Twins



HISTORIAN DATA

Historian data from the modeled asset provides a baseline and comparative function.

EXTERNAL DATA

External data from other sources (i.e. weather, maintenance history, network traffic, etc.)

PHYSICS-BASED MODEL

Fast Fourier Transforms and physics-based equations are used to model the physical processes.

CALCULATIONS

Based on the purpose of the digital twin, the application generates the desired analysis.

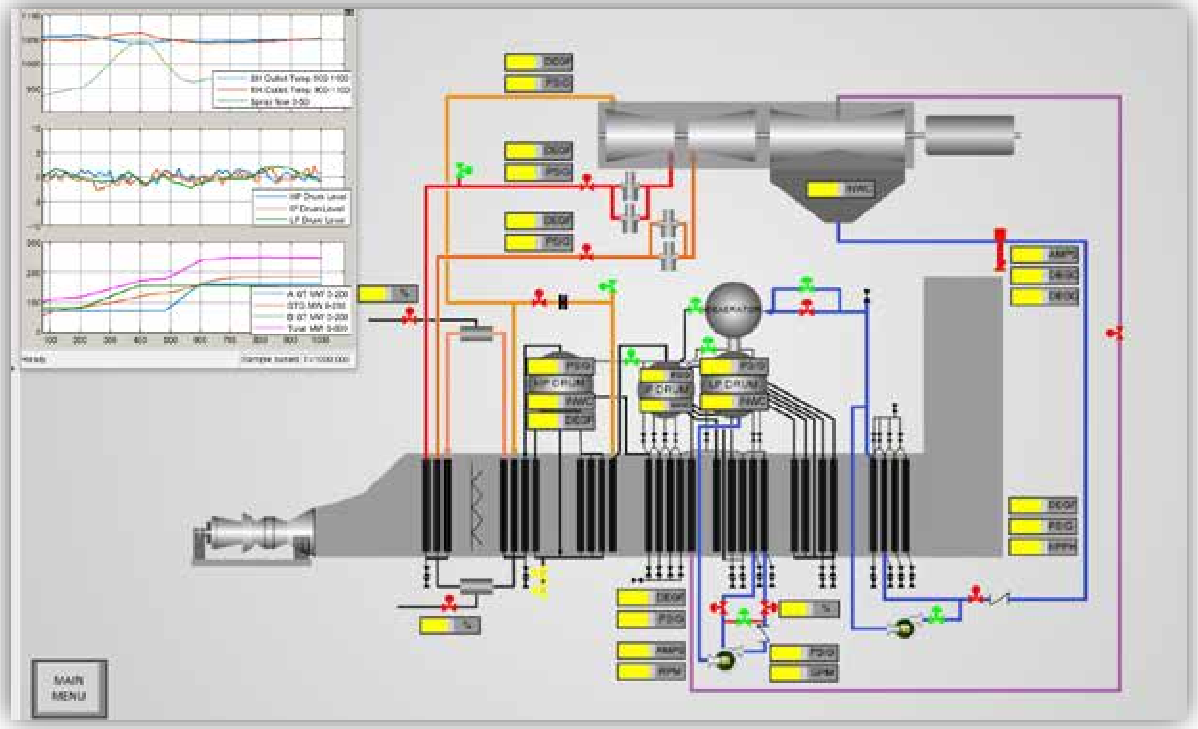
OUTPUT LAYER

Output generated for visual results or data ingestion into another application.

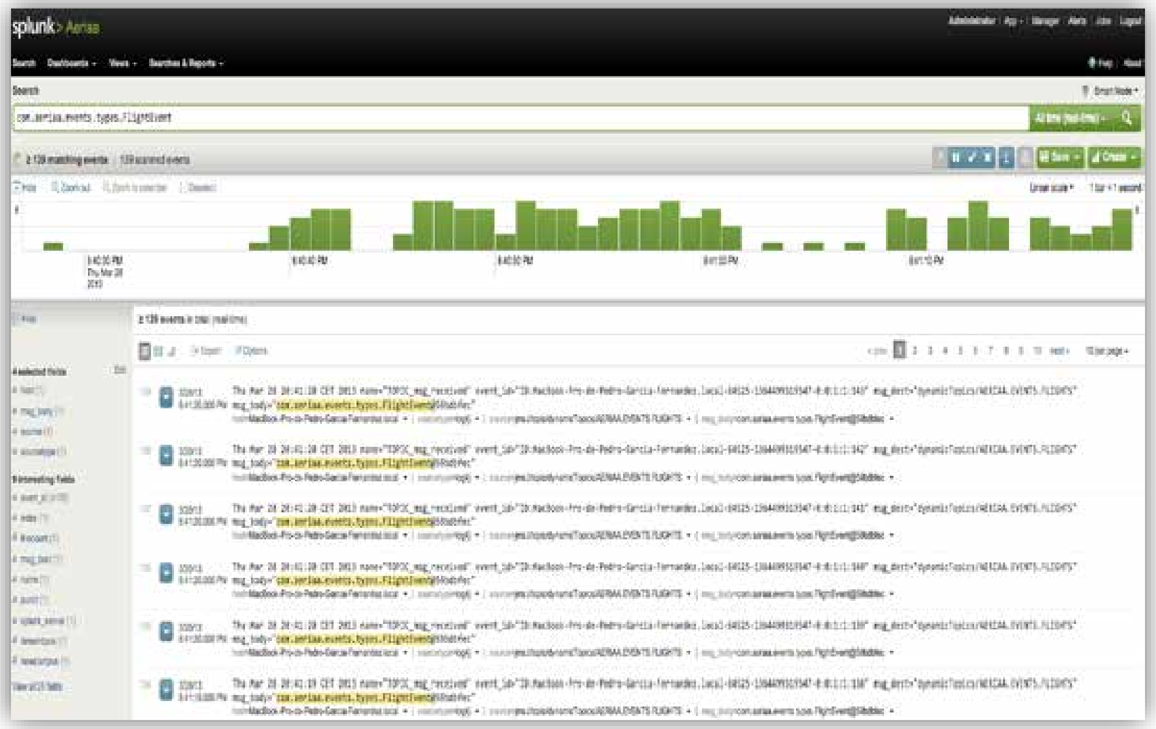
EPRI

Enhanced Detection Capability

Operational Parameters



Network Parameters



Using AI to Increase Security Response

- Through an Integrated Security Operations Center (ISOC)
  - IT network and security data
  - OT network and security data
  - Physical security system data
  - Monitoring & Diagnostic center data

- Automated response to anomalous events
  - Security Orchestration, Automation, and Response (SOAR)
  - Security operations implications (efficiency, cost, resources, etc.)

Expert System Deployment
EPRI’s LLM: STELLA

Storage **T**echnologies for **E**nergy **L**arge **L**anguage **A**pplication (STELLA)

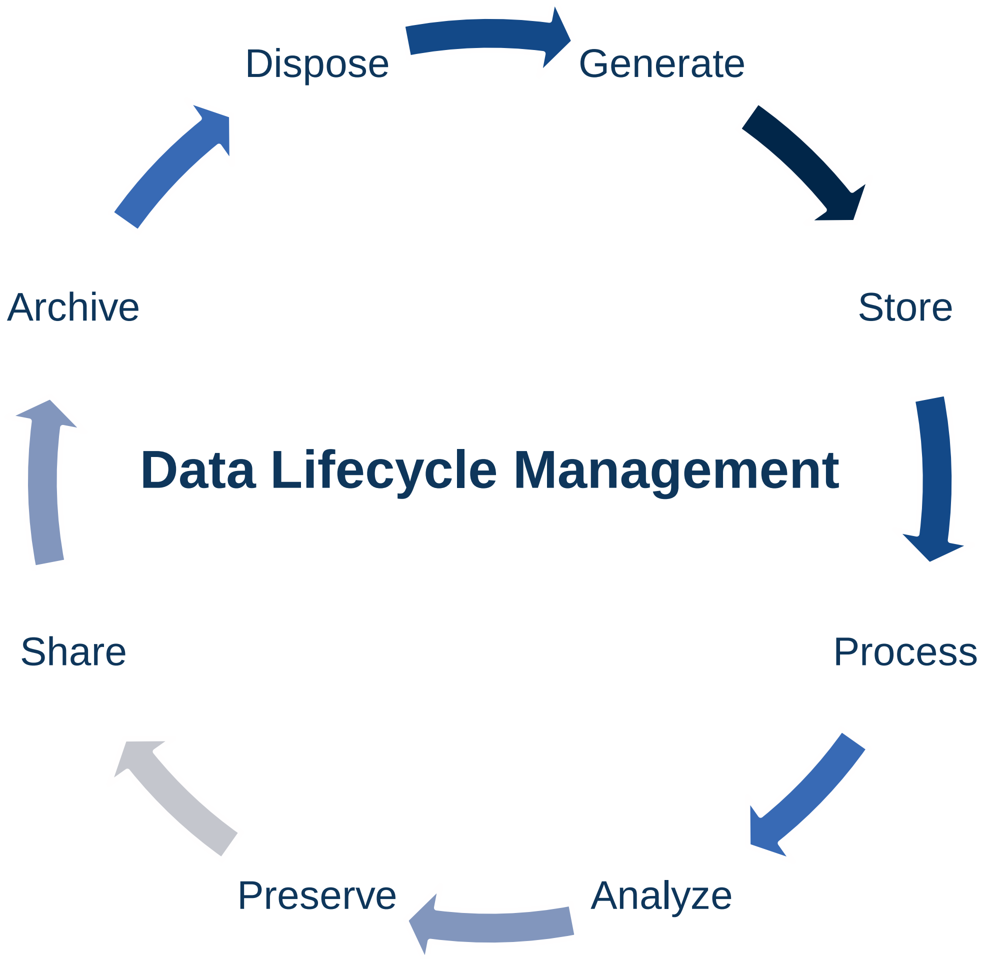
Language-based LLM built on Llama2 7B, hosted on-prem with NVIDIA DGX2 compute.

Focused on energy storage technologies (batteries, thermal, chemical, etc.)

Better performance metrics than major competitors because it is trained using *Grounding*.

Securing the Future of AI

Protecting IT/OT Data Systems



Data Lifecycle Management

Generate

Store

Process

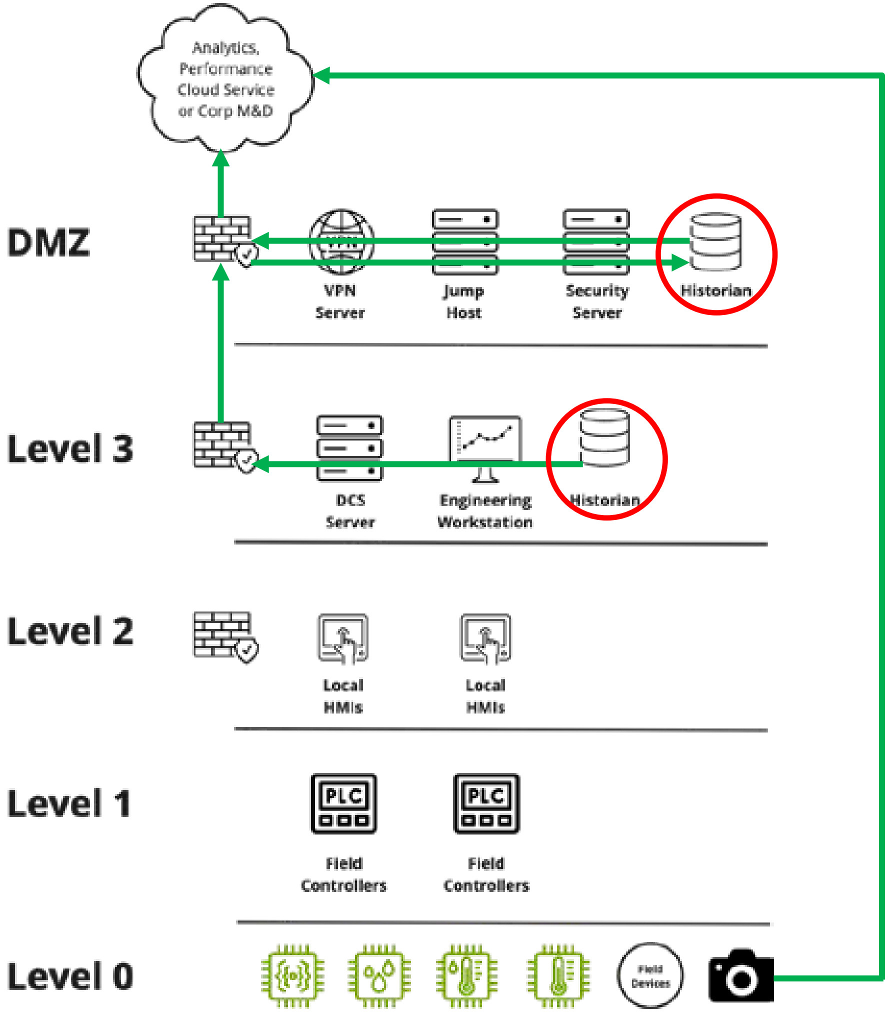
Analyze

Preserve

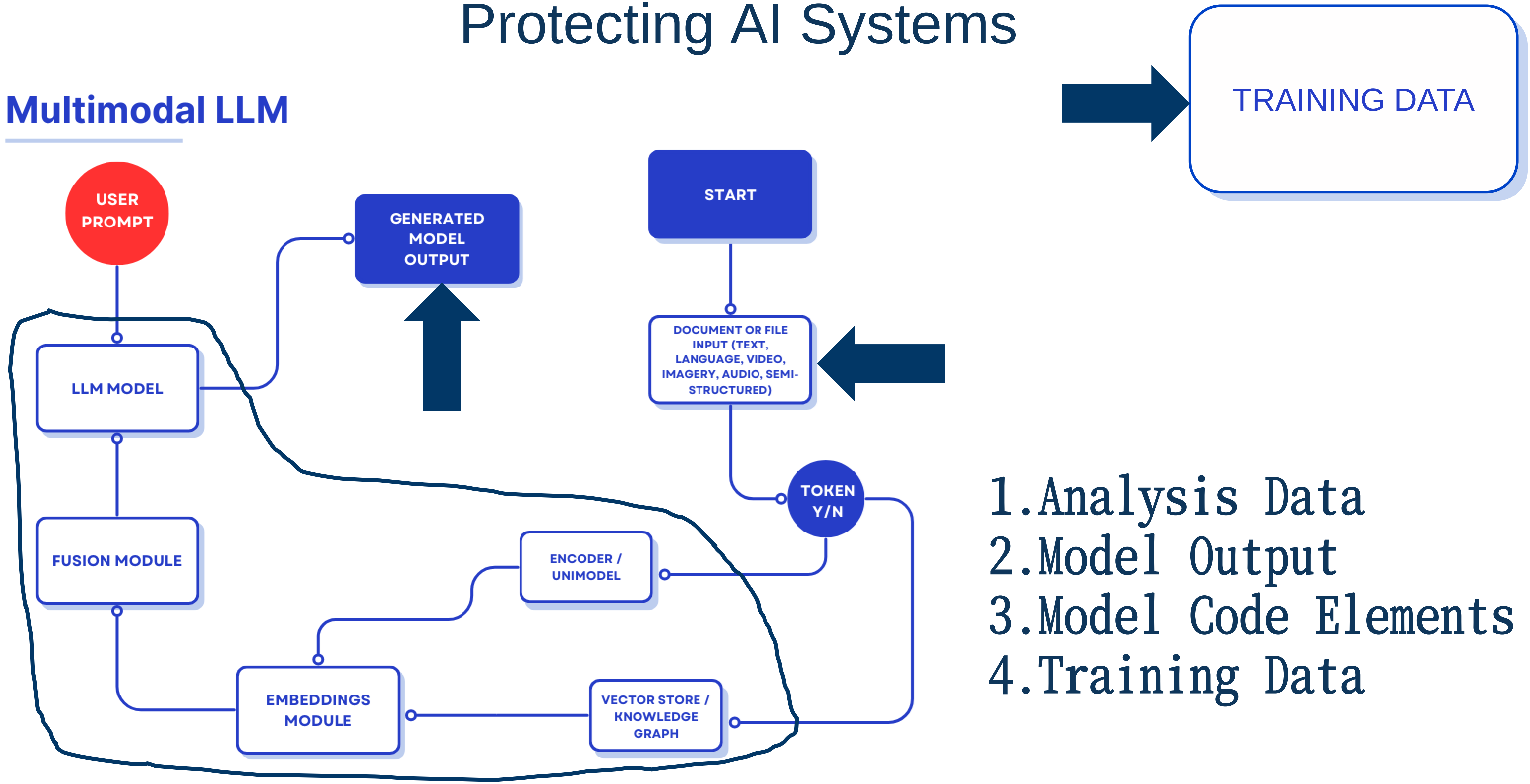
Share

Archive

Dispose



Protecting AI Systems



1. Analysis Data
2. Model Output
3. Model Code Elements
4. Training Data

Cyber Security Best Practices for AI

Secure Deployment

- Ensure robust IT governance and secure configurations in the deployment environment.
- Apply security best practices to AI systems and their IT environments.
- Manage deployment environment governance and ensure a robust architecture.
- Harden deployment environment configurations and protect networks from threats.

Continuous Protection

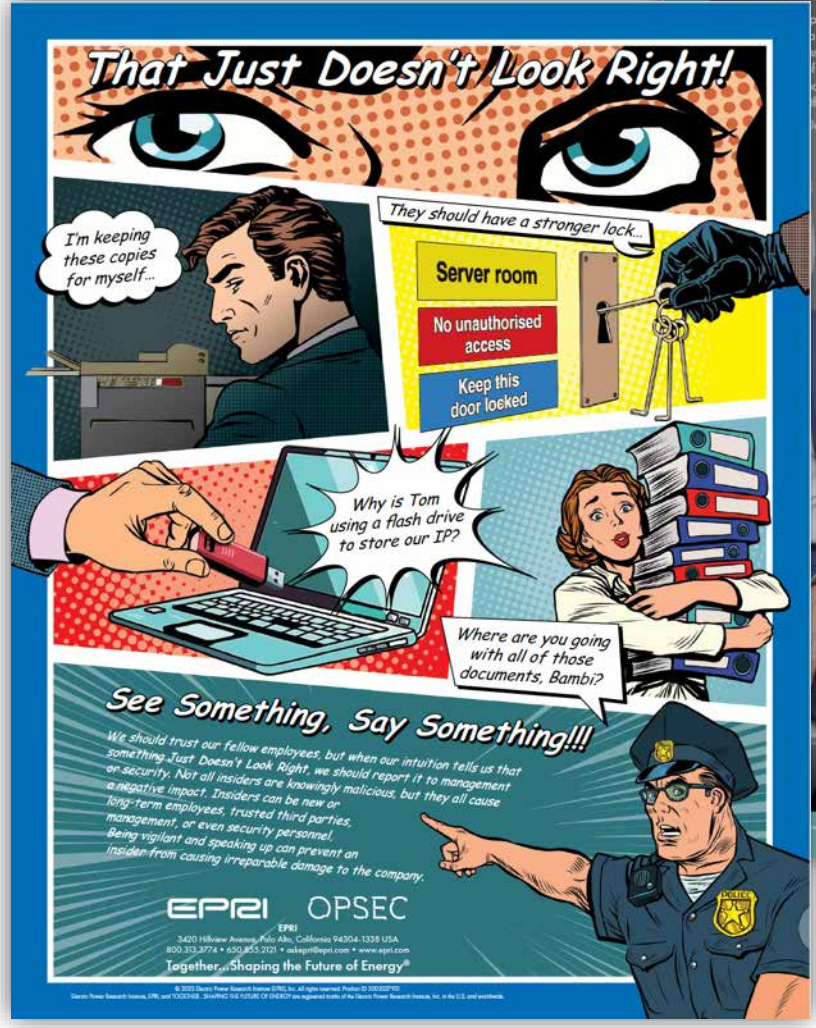
- Validate AI systems before and during use.
- Protect deployment networks and exposed APIs.
- Actively monitor model behavior and protect model weights.
- Apply and monitor cyber controls along the entire data lifecycle.

Secure Operations & Maintenance

- Enforce strict access controls and ensure user awareness and training.
- Conduct audits and penetration testing.
- Implement robust logging and monitoring.
- Regularly update and patch systems.
- Build out robust recovery and restoration plans.

Protecting Against AI Assisted Threats (Pillar 3)

- Education and Awareness
- Enhanced Detection
- Automation
- Preparedness

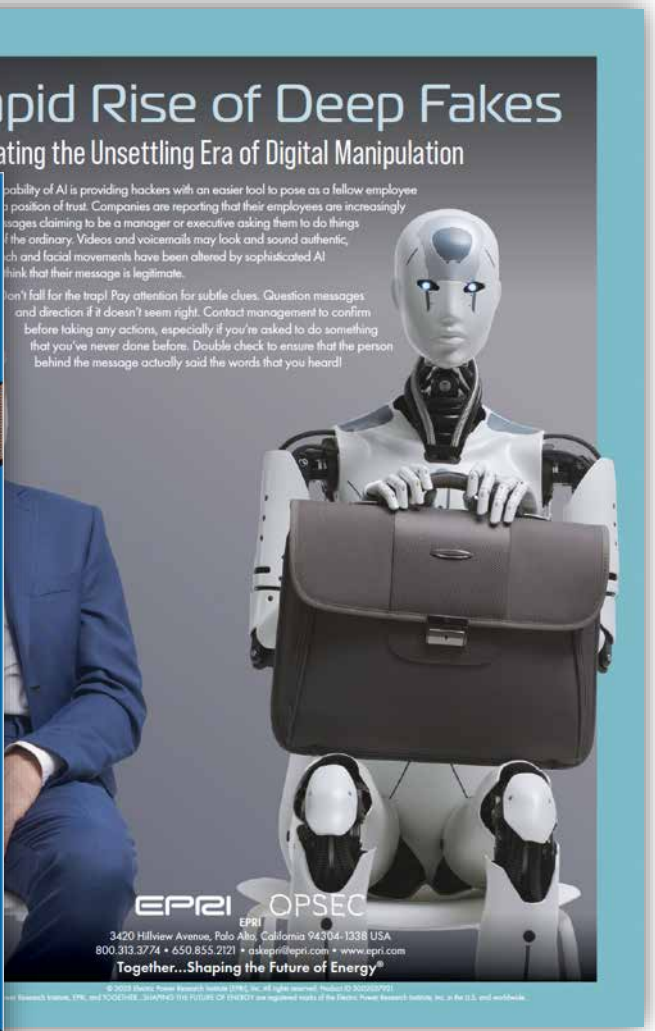

That Just Doesn't Look Right!
I'm keeping these copies for myself...
They should have a stronger lock...
Server room
No unauthorised access
Keep this door locked
Why is Tom using a flash drive to store our IP?
Where are you going with all of those documents, Bambi?

See Something, Say Something!!!

We should trust our fellow employees, but when our intuition tells us that something Just Doesn't Look Right, we should report it to management or security. Not all insiders are knowingly malicious, but they all cause a negative impact. Insiders can be new or long-term employees, trusted third parties, management, or even security personnel. Being vigilant and speaking up can prevent an insider from causing irreparable damage to the company.

EPRI OPSEC

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com
Together...Shaping the Future of Energy®



Rapid Rise of Deep Fakes

Navigating the Unsettling Era of Digital Manipulation

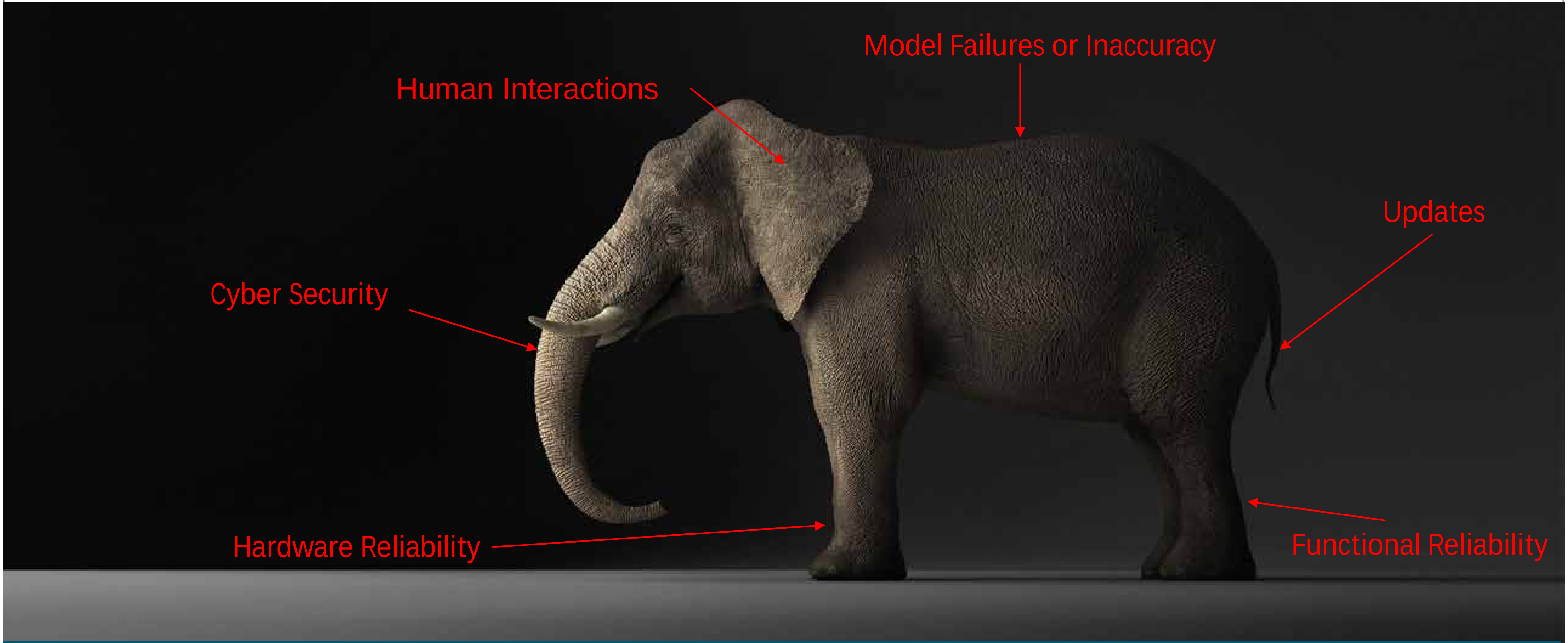
pability of AI is providing hackers with an easier tool to pose as a fellow employee
position of trust. Companies are reporting that their employees are increasingly
ssages claiming to be a manager or executive asking them to do things
f the ordinary. Videos and voicemails may look and sound authentic,
ch and facial movements have been altered by sophisticated AI
hink that their message is legitimate.

on't fall for the trap! Pay attention for subtle clues. Question messages and direction if it doesn't seem right. Contact management to confirm before taking any actions, especially if you're asked to do something that you've never done before. Double check to ensure that the person behind the message actually said the words that you heard!

EPRI OPSEC

EPRI
3420 Hillview Avenue, Palo Alto, California 94304-1338 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com
Together...Shaping the Future of Energy®

Looking at the Whole Elephant



How to address design requirements, risks, and hazards in one integrated process

Learn More About Our Work in AI at EPRI

ChatGPT and the Power Sector: What's Hype? What's Possible?

- White paper with initial considerations and potential use cases
- Published April 2023

ChatGPT and the Power Sector: What's Hype? What's Possible? – One Year Later

- White paper with revised considerations and proof-of-concept use cases
- Expected to be published by Q3 2024

Embracing the Power of Large Language Models: Shaping the Future of AI

- EPRI *Current* podcast with Christine Lee and Lea Boche
- Published September 2023

Harnessing AI to Transform Cybersecurity Detection and Response in OT Environments

- Collaborative presentation with Jeremy Lawrence
- GTC 2024

Leveraging GPUs to Coordinate Outage Scheduling for Utilities

- Collaborative presentation with Adam Wigington
- GTC 2022

Resources

- OWASP LLM Top 10: https://owasp.org/www-project-top-10-for-large-language-model-applications/
- Five Artificial Intelligence Grand Challenges for the Electric Power Industry: https://www.epri.com/research/products/000000003002022804
- Cyber Awareness Posters: https://www.epri.com/research/programs/112046/results/3002027921
- Quick Briefs (Support): https://www.epri.com/research/programs/112046/results/

Session Name

THANK YOU

Please take a few minutes to complete a short survey about this session. Your feedback will help us improve future programming for JETC.

conferences i/o

or browse to

jetc.cnf.io

Cyber Resilience in AI-Driven Industrial Control Systems: Strategies and Innovations

- Jeremy Lawrence, jlawrence@epri.com
- Jason Hollern, jhollern@epri.com