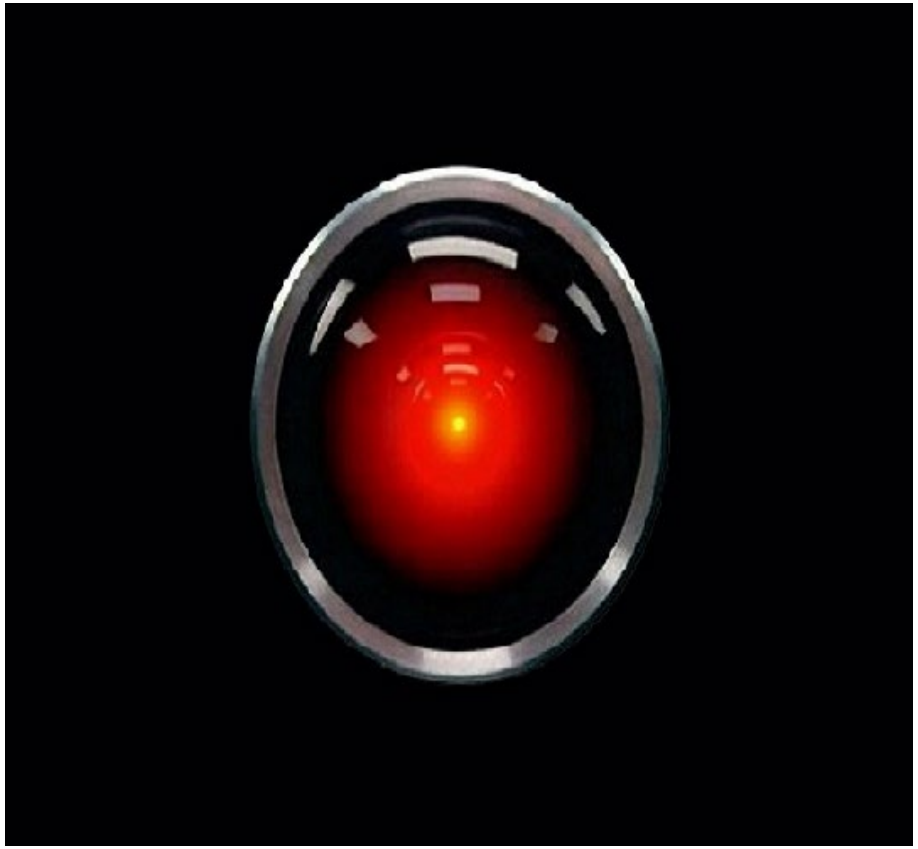
WELCOME

6-10-26 NAESB Meeting

AI in the Energy Supply Chain:
Standards, Security, and Operational Integrity

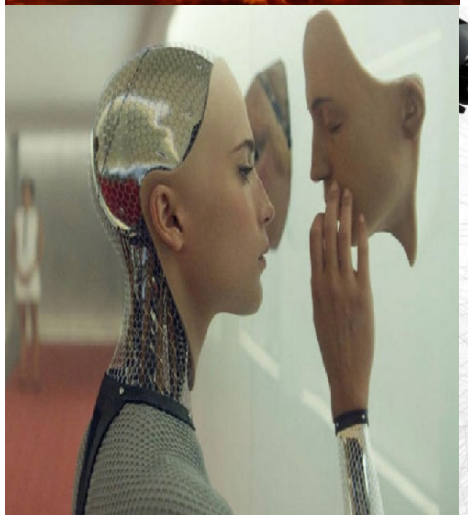
Michael Holko
Director of Cybersecurity Compliance and Oversight
Pennsylvania Public Utility Commission

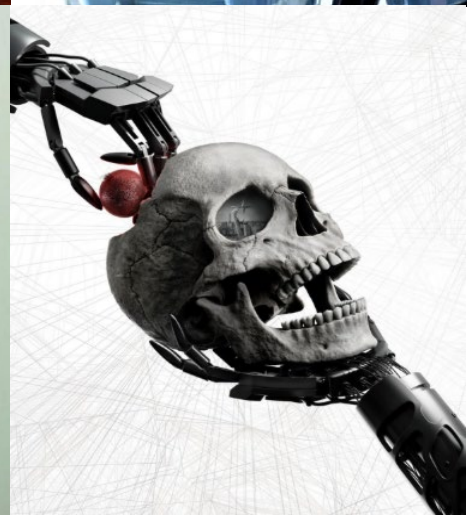
Agenda



- Welcome
- Why We Fear Artificial Intelligence
- Artificial Intelligence Overview
- Artificial Intelligence Benefits to Electric and Gas Companies
- Artificial Intelligence Threats to Electric and Gas Companies
- What Electric and Gas Companies Need to Know
- Biography and Contact Information

Science Fiction Themes





- **Nuclear Holocaust/End of the World**: Movies like The Terminator, War Games, Colossus, etc. where AI become self-aware and starts a nuclear attack or a robotic war to wipe out humanity.
- **Rogue Creation**: TV shows like Battle Star Galactica and Westworld warn us about how robots could turn on their human creators.
- **Manipulative Operating System**: Movies and TV shows like Her, Star Trek, and Person of Interest where an AI operating system becomes so emotionally and intellectually advanced that its human companion's reality is altered and manipulated.
- **Sociopathic**: Movies and TV shows like in 2001: A Space Odyssey, the AI HAL 9000 turns against its human crew with chillingly calm logic after perceiving them as a threat to its mission.
- **Singularity**: Movies and TV shows like the Matrix, Ex Machina, and Black Mirror where AI surpasses human intelligence and can improve itself, suggests that humanity will eventually be superseded, making our existence irrelevant.

News and Social Media Influence

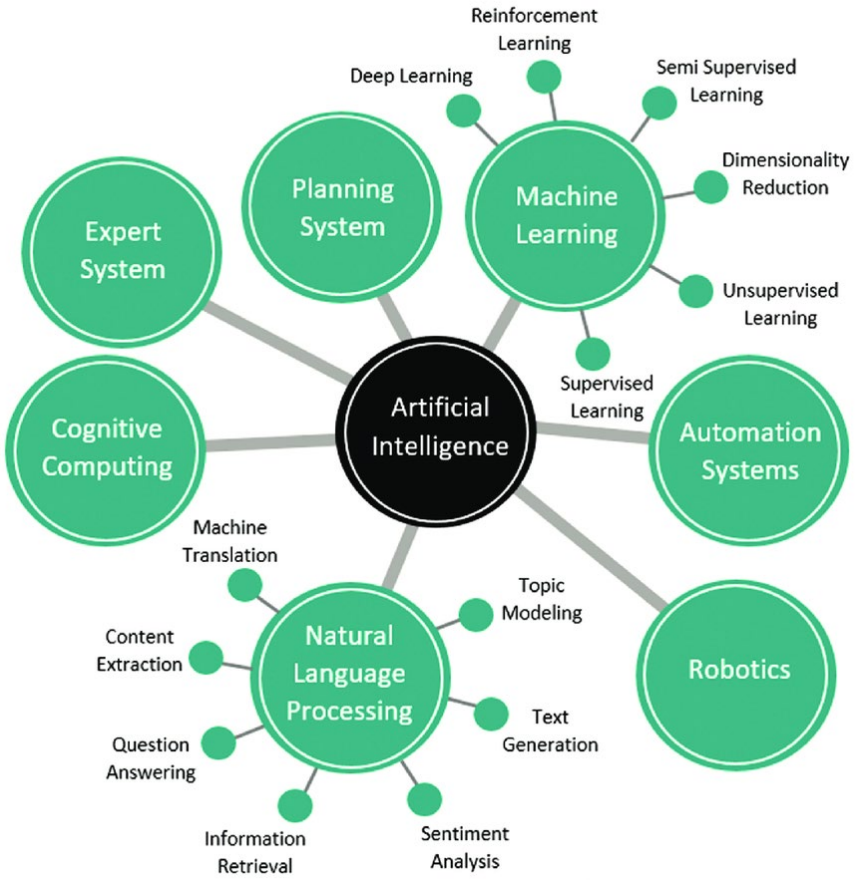
- **Sensationalism**: Headlines that inflate technological threats to grab attention. Stoking anxieties about job losses and threats to humanity. Journalists and social media bloggers frequently highlight worst-case scenarios, such as massive job losses or data breaches, without providing the necessary context or mentioning the potential for new opportunities created by the technology.
- **Fear Mongering**: Media often focus on AI's potential dangers rather than its positive applications.
- **Misuse of AI Technologies**: AI-generated fake news and deepfakes created by people become sensational news and the media uses a few instances of misuse of the technology to highlight the most terrifying possibilities of the technology which increases public distrust in AI.
- **Misrepresenting Capabilities**: Media and social media often embellishes AI capabilities. This creates a public perception of an "all-powerful" technology that is much more advanced and threatening than it truly is.

Artificial Intelligence Overview

Artificial intelligence (AI) is a field of computer science dedicated to creating machines that can perform tasks that typically require human intelligence. Rather than following explicit, step-by-step instructions like traditional software, AI systems are designed to learn and adapt from data.

In simple terms, artificial intelligence works by training a computer to analyze vast amounts of data to identify patterns and make predictions. This is often done using machine learning, where algorithms process data to find correlations and relationships.

Artificial Intelligence Overview



The process for most modern AI, particularly machine learning, can be broken down into three key steps:

- **Collect and Prepare Data**: An AI system's learning begins with a massive and diverse dataset, which can include images, text, numbers, or videos. For example, to teach an AI to recognize a cat, you would provide it with thousands of labeled images of cats and other animals.

- **Train the Model**: Using a learning algorithm, the AI processes the data to find and learn patterns. It finds the underlying features that distinguish a cat from other animals on its own. The more data it is given, the better it becomes at recognizing the patterns.

- **Predict and Improve**: Once the AI is trained, it can make predictions or decisions based on new, unseen data. It continuously refines its own internal settings to minimize errors and improve accuracy over time.

Traditional AI vs. Generative AI

Feature	Artificial Intelligence (Traditional AI)	Generative AI
Primary Goal	To analyze, categorize, and interpret existing data to solve specific problems and make predictions.	To create entirely new content, such as text, images, music, or code, based on learned patterns from its training data.
Core Function	Predictive analysis, classification, and automation of tasks. It makes decisions within predefined rules.	Content generation and creative tasks. It produces unique and original output rather than simply identifying existing patterns.
How it Works	Uses various techniques like supervised and unsupervised machine learning to find structure in data. It often follows a more transparent, interpretable decision-making process.	Uses large, complex models, like deep learning with neural networks, to learn the underlying structure of data and generate new data that has similar characteristics.
Common Uses	Spam filters, fraud detection, recommendation engines (e.g., Netflix), and predictive analytics.	Writing articles, creating images from text prompts, composing music, and generating code.
Data Needs	Depending on the task, it can be efficient even with smaller, more specific datasets.	Often requires massive, diverse datasets to learn how to create high-quality, novel outputs.
Key Limitation	Its output is limited to what it has been trained to recognize or classify. It cannot produce original content beyond its existing data.	It can "hallucinate" or create false but plausible information, and its creative output lacks true human understanding or intent.
Data Requirements	Needs structured, high-integrity Scada Data to predict failures.	Can process unstructured safety manuals or field logs but requires strict operational “fences” to prevent hallucinations.

Artificial Intelligence Benefits to Electric and Gas Companies

Benefits for Electric Companies

- Grid Reliability & Predictive Maintenance: AI algorithms analyze sensor data from substations and transformers to predict equipment failures before they happen. This can reduce maintenance costs by up to 56% and increase profits by 3–4%.
- Operational Efficiency: Autonomous drone missions for grid inspections can reduce inspection time by 50–90% compared to manual helicopter flyovers or patrols.
- Load Balancing & EV Integration: AI helps manage the surge in demand from electric vehicles (EVs) by predicting charging patterns and incentivizing off-peak usage through dynamic pricing.
- Renewable Energy Integration: Machine learning models forecast wind and solar production, allowing grid operators to better integrate intermittent power sources.

Benefits for Gas Companies

- Leak Detection & Safety: AI-powered optical gas imaging (OGI) systems automatically detect and mitigate methane leaks, improving safety and environmental compliance.
- Supply & Demand Synchronization: AI analyzes market data and weather patterns to provide more accurate demand forecasting, helping producers align supply chains and minimize waste.
- Optimized Power Generation: AI tools target heat rate efficiency improvements in gas-fired plants, potentially saving millions in fuel costs annually.
- Infrastructure Support for AI: Natural gas is recognized as the fastest solution to power the massive energy demand of AI data centers, providing the 24/7 reliability that intermittent renewables may lack.

Artificial Intelligence Benefits to Electric and Gas Companies

Holistic Security Overview

- IT/OT Convergence: AI unifies data from both IT and OT networks, providing a single, comprehensive view of the security landscape. This bridges the communication gap between security teams and improves coordinated responses.

Automated Response and Resilience

- Automated Incident Response: AI-powered Security Orchestration, Automation, and Response (SOAR) tools can automatically contain a threat by isolating endpoints or blocking malicious activity, reducing incident response time.
- Simulations and testing: Using digital twins, AI can simulate cyberattacks in a virtual environment to test security measures without disrupting real-world operations.

Enhanced Threat Detection

- Anomaly Detection: AI algorithms establish a baseline of normal network activity to instantly flag unusual behavior in both IT and OT systems, such as unauthorized commands on a SCADA network.
- Forecasting attacks: AI analyzes threat intelligence and historical incidents to predict potential attack vectors, enabling companies to proactively reinforce defenses.

Improved Operational Technology (OT) Defense

- Asset Visibility: AI automatically identifies, and maps all connected devices across the OT environment, removing blind spots and securing every endpoint.
- Zero-trust Security: AI continuously verifies access requests from both users and machines, enforcing strict, least-privilege access to critical systems.

Strengthened Physical Security

- AI-powered Surveillance: AI video analytics monitor physical assets like substations, detecting unusual behavior, unauthorized access, or abandoned objects, and alerting security in real time.

Artificial Intelligence Threats to Electric and Gas Companies

- **Automated and Enhanced Reconnaissance**: AI enables attackers to scan for vulnerabilities across vast IT and OT networks at machine speed.
- **Sophisticated Social Engineering**: Generative AI creates hyper-personalized phishing emails that are difficult to distinguish from legitimate messages. AI can analyze publicly available information to identify key personnel and third-party suppliers to target.
- **Deepfakes**: Deepfake voice and video can be used to impersonate executives or engineers, tricking employees into unauthorized actions.
- **Advanced Operational Technology (OT) Attacks**: Attackers use "adversarial machine learning" to subtly manipulate data fed into OT systems, causing them to fail or malfunction.
- **Malware**: AI-driven malware can learn to evade traditional detection methods, infecting critical control systems unnoticed.
- **Data Analysis**: AI can analyze system data to precisely time an attack for maximum disruption, such as a targeted equipment failure during peak demand.
- **Combined Attacks**: AI can combine with other technologies like drones to target physical infrastructure, such as substations, from a remote location.

What Electric and Gas Companies Need to Know

Standards for AI Operations

- **Establish Clear AI Governance**: Electric and gas companies need to confirm that they have a formal AI governance framework in place. This framework should establish policies and ethical guidelines for the responsible development and use of AI, as advocated by national frameworks from organizations like the National Institute of Standards and Technology (NIST).

- **Identify Decision-making Boundaries**: AI models can be complex and opaque, making it difficult for stakeholders to understand their decisions. Electric and gas companies need to be able to disclose to stakeholders and regulators how AI is being used in critical, customer-facing decisions, such as rate adjustments or service disconnections.

- **Ensure Accountability**: In the event of a system error or failure, electric and gas companies must ensure accountability is defined. You need to be clear who is responsible for the performance, ethics, and safety of AI-driven systems.

What Electric and Gas Companies Need to Know

Stakeholder and Regulator Equity and Bias

- **Prevent and Audit for Bias**: If trained on biased historical data, AI can inadvertently perpetuate or amplify existing inequities. Electric and gas companies should be able to tell stakeholders and regulators how they are auditing their AI models to prevent discriminatory outcomes in pricing, resource allocation, and customer service.
- **Ensure Transparency**: Electric and gas companies should be able to provide clear, accessible explanations of how AI is used and how customer data is protected. This builds trust and transparency, especially regarding automated decisions that affect customers, stakeholders, and regulators.

Cybersecurity and Data Management

- **Mitigate New Threat Vectors**: AI can expand an electric and gas companies attack surface and introduce new risks, such as data poisoning and model manipulation. Electric and gas companies should be able to articulate AI models from known AI exploits such as Data Poisoning, Data Manipulation, Prompt Injections, etc.
- **Protect Sensitive Data**: Electric and gas companies collect vast amounts of customer data through smart meters and other technologies. Electric and gas companies need to verify that robust cybersecurity protocols and data governance policies are in place to prevent data breaches, protect customer privacy, and ensure compliance with regulations.

What Electric and Gas Companies Need to Know

Operational Reliability and Safety

- **Monitor Autonomous Systems**: AI in critical infrastructure is increasingly autonomous, capable of making decisions about grid management or other utility functions. Electric and gas companies should ensure that they maintain a "human-in-the-loop" oversight process for autonomous systems to prevent unintended consequences.
- **Validate Safety-Critical Models**: When AI is used for safety-critical functions like predictive maintenance, electric and gas companies should audit and validate the AI models function and usage. This ensures that the AI can be trusted to perform its intended function without risking catastrophic failure.
- **Evaluate Cost-Benefit**: Electric and gas companies should justify the financial investment in AI initiatives to stakeholders and regulators, detailing how the technology improves efficiency, reliability, or service. Regulators can scrutinize the ROI to ensure ratepayer costs are justified.
- **Address Workforce Changes**: The adoption of AI will likely change roles for the current workforce. Electric and gas companies may want to examine their AI implementation strategies to determine the impact to their workforce.

Biography and Contact Information

Michael C. Holko was appointed as the first Director of the Office for Cybersecurity Compliance and Oversight (OCCO) by Chairman Gladys Brown Dutrieuille in September 2018. OCCO is the Pennsylvania Public Utility Commission's office responsible for working with the regulated utilities to ensure they have adequate measures in place to help prevent and/or mitigate damage from cyberattacks on their critical infrastructure.

As the Director of OCCO, Mr. Holko is responsible for advising the Chairman, Commissioners, and Executive Director on policy and procedural issues; leading cybersecurity investigations; implementing improvements involving cybersecurity oversight functions of regulated utilities; drafting proposed cyber-related regulations; and overseeing the preparation of orders, rulemakings, policy statements, Secretarial Letters and memoranda related to cybersecurity regulations of the regulated utilities.

Michael Holko, Director, Office of Cybersecurity Compliance and Oversight
Pennsylvania Public Utility Commission
400 North Street, 3rd Floor North
Commonwealth Keystone Building, HBG, PA 17120
717-425-5327 | miholko@pa.gov