



AI and Energy: Network Innovation and Growth

**This article was also published in Pratt's Energy Law Report's June 2024 edition.*

Apr 09, 2024

Categories:

[Publications](#)

[Technology Blog](#)

Authors:

[Gene F. Price](#)

[Lauren E. Cole](#)

[Janelle E. Thompson](#)

This is the fourth in a series of articles outlining successful approaches for businesses integrating artificial intelligence (AI) while minimizing its potential risks. Here, we examine the application of AI in connection with information technology (IT) and operational technology (OT) networks supporting the energy industry. The manufacturing and energy industries are somewhat unique in that their operations often depend on OT networks, which in turn usually rely on their IT network to operate accurately. AI has the potential to increase the efficiencies of both, but success with [enterprise AI depends on strong governance](#), including appropriate policies, procedures, and risk management.

What Are OT and IT Networks?

IT networks connect resources on a grid of network nodes for data to be communicated. By comparison, OT networks control, process, and monitor operational data for industrial processes and devices. Energy providers rely more heavily on OT networks to control and isolate processes and increase security. Recently, the industry has seen an increase in IT/OT “network convergences,” where OT networks communicate with IT networks to increase efficiency. AI can mitigate IT/OT interoperability risks and increase efficiency by targeting vulnerabilities, reducing waste, and improving business infrastructure, provided that proper governance procedures are in place.

What Inefficiencies Can AI Reduce?

Particularly when partnered with IT sensors, AI is increasingly more vital to both centralized and intermittent energy sources, including oil and gas, as well as energy from renewable resources.

AI Can Reduce Waste and Cost

Transitioning to an AI-centered system will allow for more complex energy systems and efficient energy resource allocation. Total reliance on AI without human oversight or sufficient training could expose businesses to risks from inaccuracy or non-compliance with new industry regulations. However, if done with the proper protocols in place, the billions of data points produced annually by alternative energy sources can be collected and more easily analyzed by AI. Flaws in pipes, wiring, and machines can be costly fixes for utility companies, both in expenses and brand reputation with customers. Features like AI image recognition could also analyze photos and videos of energy facilities to alert employees about potential failures, reducing risk and maximizing financial returns from the reduced downtime.

AI Can Reduce the Risk of Grid Failures

AI can assist with predictive maintenance in power grid inspections, anticipating when environmental conditions may become harmful, evaluating the ongoing performance of energy assets, and monitoring general “wear and tear,” all when properly trained and supervised.

Renewable energy assets such as wind turbines and solar panels often face extreme weather and are in remote locations of the country. Companies are using AI to predict when a machine fault is likely to happen in real time, allowing for quicker responses and resolutions.

AI forecasting tools can also monitor performance to identify potential inefficiencies and faults before they happen, including within customer equipment. Lastly, AI can predict the supply and demand of energy usage, allowing companies to reasonably anticipate peak energy use and reduce electricity outages.

AI Can Address Cybersecurity Vulnerabilities

OT networks have historically been preferred for their security-based isolation from other networks. However, advances in

technology have led to cyber-attacks that take advantage of outdated models used by OT networks. Hackers have infiltrated critical infrastructure networks by planting malware in OT networks, causing corruption to system processes. When connected to IT and exposed to the internet, older OT models remain highly vulnerable as advanced hackers spot vulnerabilities to exploit. While convergence of IT/OT networks has created efficiencies, OT network vulnerabilities have increased despite the safeguards IT networks may have in place.

Another concern is that AI can be trained to attack OT networks. Volt Typhoon hackers from Beijing infiltrated critical infrastructure in Guam and the United States for over five years until recently discovered by the FBI and NSA. The hackers in this attack used AI to recruit assets, steal secrets, and rapidly process the information AI collected.

To cope with this development, AI can be incorporated into incident response plans used to address and alert businesses to anomalies. AI models can be trained for risk prioritization to trigger the best response protocols (in a model more advanced than a code stating “if X then Y” as the AI learns and adapts over time). Further, any anomalies detected by AI can be reported in simplified formats that help security teams manage threats while reducing business efforts to track such detections. Because AI can anticipate cybersecurity weak spots in OT networks, new policies and procedures that effectively address AI as both a tool and a threat can limit the very risks created by AI.

Conclusion

The use of AI in the energy industry will only increase as more organizations seek to diversify, strengthen, and grow their energy assets. Whether a company is considering an initial investment in an AI product, or already has a robust AI program in place, establishing a comprehensive AI governance strategy is critical to a successful outcome. The professionals at Frost Brown Todd are committed to providing guidance regarding AI governance, regulatory considerations, and more. If you have questions, please contact the authors or any attorney with our [Artificial Intelligence](#) team.

AI Legally Speaking

Explore the collection of articles below for more AI-related coverage and legal analysis.

- [**Managing Data Security and Privacy Risks in Enterprise AI**](#)
- [**New Expectations for AI: Governance is Key for AI Success in Health Care**](#)
- [**USPTO Guidance Suggests Two Strategies for AI Inventions**](#)
- [**FTC's New Rule on Consumer Reviews: Ensuring Compliance with Human- and AI-Generated Content**](#)
- [**Decoding Colorado's Artificial Intelligence Act**](#)
- [**Investment Management + AI = New Opportunities, Unique Risks**](#)
- [**AI Chatbots, Hallucinations, and Legal Risks**](#)
- [**AI and Health Care Providers: Managing the Risks with Data**](#)
- [**Using Generative AI in Manufacturing: Three Key Considerations**](#)
- [**Will AI Destroy the DMCA Copyright Compromise?**](#)
- [**Three Steps to AI Success for CEOs**](#)

[Learn More](#)

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.