Paradigm

How AI Is Reshaping Risk Management in Energy Industry: A Qualitative Study of Leading Companies

Delia IACOB*
Bucharest University of Economic Studies, Bucharest, Romania
Corresponding author, delia.iacob79@yahoo.com

Abstract. *This article examines the applications of artificial intelligence (AI) in risk management process in energy sector and the emergent adoption patterns across subsectors. The paper focuses on practical and observable deployments, building on recent academic work that frames AI as a driver for the energy transition while also highlighting governance, data and cybersecurity concerns. A dataset of 50 AI use-case instances was compiled and assessed, employing a structured content analysis, which were gathered from public data available for leading energy companies. Each case was coded according to four risk management stages (identification, analysis/assessment, prediction and mitigation/treatment), a primary AI capability class (e.g. predictive maintenance, forecasting/optimization, computer vision inspection, digital twins, robotics, neuro linguistic programming (NLP)/Generative AI, cybersecurity analytics) and a dominant risk-control archetype (e.g. reliability control, inspection at scale, resilience forecasting and response optimization, operational decision support).The results suggest that AI is most frequently integrated into mitigation pathways rather than utilized as a standalone analytics layer. There are two primary patterns that emerge: (1) reliability oriented solutions that focus on time-series anomaly detection and predictive maintenance, which connect sensor signals to maintenance actions and (2) resilience and inspection oriented solutions, particularly in utilities and nuclear contexts, that prioritize interventions and reduce exposure to hazards by utilizing forecasting/optimization and computer vision/robotics methods. Subsector comparisons demonstrate domain-specific risk fit: upstream / offshore prioritize reliability control and digital twins; utilities prioritize resilience forecasting and inspection at scale; and refining/downstream prioritize decision support and compliance-linked use cases. The results indicate that the value of AI in risk management is the reduction of the detection to action cycle. Equally, to progress on the automation maturity, it is necessary to improve cybersecurity governance, transparency and validation.*

Keywords: Risk Management, Artificial Intelligence, Energy sector, Risk Control, Operational resilience.

Introduction

AI is positioned as a transformative capability in the energy industry, facilitating the broader net zero transition, operational efficiency and reliability. The most recent literature highlights the importance of AI-enabled forecasting, optimization, hybrid systems and cybersecurity enhancements. However, it also cautions that the adoption of these technologies may present challenges in the areas of data quality, model bias, opacity, privacy, interoperability and systemic risk. Parallel to this, institutional and regulatory perspectives present AI as both risk reducer (through predictive maintenance, outage prevention and enhanced market surveillance) and a risk multiplier (through cyber vulnerabilities, overreliance, third-party concentration and rapid market dynamics under stress). This necessitates the collection of proper evidence regarding the operationalization of AI in energy subsectors' risk management.

This paper bridges the gap by comparing real-world AI deployments to the stages of the risk management cycle and to tangible risk control mechanisms. The study provides cross-sector insights into areas where AI is closest to operational control and where it remains at an advisory level. This is achieved by comparing patterns across numerous energy segments using publicly

DOI: 10.2478/picbe-2026-0019

available disclosures. The primary objective is to reveal subsector specific archetypes, identify dominant AI capability, link it to a risk stage and evaluate maturity through its proximity to control.

Consequently, the research is constructed around the following research questions: how are AI use cases distributed throughout the stages of risk management cycle; in each stage of risk management which AI capability classes are most frequently employed; what are the most prevalent risk control archetypes and how do they differ by energy subsector; to what extent do these deployments approach operational risk control and what is the maturity level?

The study provides a perspective on the transition of risk management discipline from periodic manual processes to more continuous, algorithm assisted decision and actions pathways.

Literature review

After carefully reviewing reputable academic sources, but also regulatory, professional and institutional papers we can conclude that AI (Artificial Intelligence) is without doubt a transformative force in the energy industry.

Wang *et al*. (2024) conducted a consistent literature review analyzing how AI is integrated in energy transition. They observed that AI tools enhance multiple elements in the energy system, starting from acceleration of renewals adoption to improved demand management by using advanced forecasting and optimization instruments. AI makes new things possible such as hybrid energy storage and vehicle-to-grid systems. AI also plays an important role in managing cybersecurity risks and strengthening grid stability, thus supporting resilient and sustainable operations. The review also highlighted several challenges in adopting AI like data quality, ethical and privacy concerns, interoperability, but also argued that AI driven insights can make energy systems more proactive and adaptive. Their theoretical contribution is conceptual; AI is a strategic catalyst for net zero transition of energy industry.

Chen *et al.* (2024) explored how AI adoption influence companies risk taking behavior. Using panel data analysis, the authors demonstrated that AI adoption significantly increases the risk-taking levels. They also found that financial constraints and capital limitations amplify AI's effect. AI increases risk taking because it reduces manager's perception of risk, reshapes decision making process providing better information and confidence and lowers perceived risk, thus raising enterprise's risk appetite.

Shobanke *et al*. (2025) performed a systematic review of AI and machine learning (ML) in energy and climate change modeling. Key benefits include predictive analysis and optimization. By applying cluster research by application, they found that AI models (e.g. deep neural networks) can capture with a higher accuracy climate dynamics and variability outperforming traditional methods. In energy modelling, AI (e.g. Long Short-term Memory networks) delivers highly accurate short-term demand forecasts and techniques like XGBoost reveal pricing and demand insights. These predictive tools support improved operational efficiency and data driven decisions. The authors stress that AI driven predictive power can guide sustainable planning (reducing outages, optimizing grid operation). They also raise the topic of governance as very important to mitigate risks and maximize social benefits. While AI modeling is improving forecasting and decision, they are warning on the challenges of data biases and model uncertainty.

Khalil *et al*. (2005) in their paper demonstrated how combined AI and mathematical programming can lower operational risk and they proposed a practical optimization framework in a trade finance context (focused on Letters of Credit in banking environment) but this approach can be transferable to any complex process. They build a model that, based on AI generated document indices, assign verification tasks to human checkers, optimizing the way these assignments are made and balancing efficiency and risk (their model reduced operational risk by

68.3%, improving compliance and minimizing errors). The main point is that AI and optimization work better together – AI processes the data, flagging problems, while optimization adds human review in places where it will lower the risk the most.

Milojević and Redžepagić (2021) present a qualitative analysis of AI and ML (machine learning) applications in banking risk management. Their focus is on financial sector risk categories (credit, market, liquidity, operational risk), however their work can have wider implications for risk management frameworks. They argue that AI and big data tools have growing influence and the capacity to enhance risk management universally. They emphasize credit risk as a primary area of AI application (e.g. advanced credit scoring algorithms) while also acknowledging that AI may improve stress testing, monitoring and capital requirement assessment. The authors conclude that calibrated and adequately prepared applications of AI/ML can produce beneficial effects on credit, market, liquidity, operational risk and others. This approach is rather conceptual than empirical, synthesizing practical examples and literature. The main idea is that AI/ML enhances traditional risk models by identifying pattern in extensive datasets.

Gubareva *et al.* (2025) utilize econometric risk analysis to examine financial and energy markets, focusing on the interactions between the crude oil market, AI/technology sectors and green technology sectors. They use a new quantile-on-quantile connectivity method on data from 2018 to 2023 to explore how severe ("tail") risks move between markets. The main results show that markets associated with stock and AI are usually net risk transmitters, while traditional assets markets like crude oil and the US dollar can help protect against shocks coming from IT (Information Technology) and AI sectors. The approach (tail dependence analysis) and results show how investments in new technologies could influence systemic risk in energy markets and the contagion effects among cutting-edge AI indices, clean energy stocks and commodities.

Wong *et al.* (2024) examine the influence of AI on supply chain risk management and its agility in small and medium firms. Based on the resource-based view, they gather survey data from executives and use a two-stage analysis (artificial neural networks). The study reveals that using AI in risk management makes the supply chain more flexible, directly and indirectly. AI specifically improves the re-engineering capabilities. The main insight is that the use of intelligent risk tools enables dynamic adaptation, managers can simulate scenarios and reconfigure operations more quickly, and AI driven decision support (predictive modelling) enhances operational flexibility and resilience.

Velev and Zlateva (2023) examine the challenges of applying AI in disaster risk management. While concentrating on natural disasters, numerous aspects are also applicable to systemic risk contexts. They talk about the roles AI can play in disaster prediction and resource optimization, but they also raise some potential issues related to data quality, diversity of data from sensors and social media, integration of AI with existing emergency systems and major ethical and privacy concerns. They also bring up social and moral issues, like bias in algorithms or unfair access to AI tools and raise the concern that if these points are not addressed, AI could be a risk amplifier.

Biolcheva (2021) provides a conceptual analysis of the integration of AI info into conventional risk management framework. They look at each step of risk management (identification, assessment, treatment and monitoring) to see how AI fits in. The author discusses the benefits of AI, such as real-time analysis, processing large datasets, more comprehensive risk identification and increased accuracy in risk assessments. Additionally, they stress also some concerns related to loss of algorithms transparency, cyber risks and potential human anxiety about being replaced. They propose a complementary approach, AI to conduct complex analysis, while ultimate decisions are reserved to human experts. The contribution is organizational, aligning AI technologies with risk management phases and highlighting the necessity for continuous human oversight to guarantee reliability.

Pantano *et al.* (2024) present an editorial examination of the adverse implications of AI in industrial environments. They emphasize that although AI can automate tasks and enhance decision-making process, it also presents risks: predictive models might fail during crisis (as observed during pandemic period breakdowns), AI projects usually require substantial resources and end user must have confidence in technology. Very important, AI systems can maintain human biases, resulting in unethical or discriminatory results. The authors advocate for additional research to alleviate these adverse impacts (algorithmic bias, insufficient transparency, impact on workers). Their work provides a view of challenges and advise, as firms implement AI, they must proactively address these "dark"side concerns trough robust validation, ethical frameworks and consistent user trainings.

Adding to the academic reviews of AI impacts, professionals, institutions and regulators have completed the perspective as presented in the following paragraphs.

The Global Financial Stability report of International Monetary Fund (IMF) (2024) examines the impacts of AI in capital markets with implications for energy trading. The paper indicates that application of AI in energy markets is in early stages; a Dutch study observed that most trading algorithms employ just basic machine learning, frequently serving as signals for human traders. Nevertheless, AI driven trading can enhance efficiency and price transparency. By facilitating better risk management, increasing market liquidity and enhancing market surveillance by both players and regulators, AI may lower the risks to financial stability. Meanwhile, additional risks could appear such as: increased market speed and volatility under stress, particularly if AI model trading strategies all react similarly to a shock or stop working due to an unforeseen event; reliance on a small number of third party AI service providers that control the majority of the processing capacity, computational power and language model creates as well a lot of operational risks; risks related to potential interactions between various AI models used by traders in the context of activities migrations between financial providers, as well as lack of transparency and monitoring; increased risks of cyberattacks, market manipulation through fraud and misinformation in social media. While many of these risks are covered by the current regulatory frameworks, significant new and unexpected events might appear and the following mitigation directions are proposed: in light of possibly quick AI driven price movements, margining procedures should be reviewed; data collection and monitoring for big traders should be improved especially in non-banking sectors; a risk mapping from regulated entities is necessary to address reliance on data models and technology infrastructure; have a concerted strategy to identify essential third party AI service providers and improve cyber-attacks protocols in an effort to make capital markets more resilient with a consideration to over the counter markets' resilience, efficiency and integrity as well.

According to a note of International Finance Corporation / World Bank Group (2020) related to artificial intelligence in power sector, AI contributes to operational reliability and asset risk reduction. Smart meters, sensors, and phasor measurement units (PMUs) form an "information layer" that allows for real time system visibility. AI/ML is said to be especially well suited to these high volume, heterogeneous grid datasets. To lower outage risk and enhance reliability management, this analytics capability offers fault detection, predictive maintenance, power quality monitoring and renewable forecasts. Algorithmic techniques are crucial for risk monitoring at grid scale since even a modest sampling rate across one million smart meters produces incredibly massive information. This technical view is supported by a survey performed by KPMG (2023) on the use of generative AI in energy, natural resources and chemicals which demonstrates how decision makers anticipate AI to support maintenance prediction for plants and pipelines, automate routine tasks and decision processes and align operational risk reduction objectives (downtime prevention and integrity management).

RAND Europe (2024) explored the risks and opportunities of the deployment of AI applications in electricity systems. In their report, this research organization views AI as a tool for enhancing energy security outcomes, such as system performance and dependability, while arguing that benefits must be assessed considering a structured risk taxonomy unique to electrical systems. In this perspective, AI is integrated into core functions: automated decision cycles, forecasting and optimization. This shifts risk management from periodic, manual controls to continuous algorithm assisted operations. RAND offers also a sector relevant risk taxonomy identifying six major risk classes: cybersecurity breach/intrusion (including poisoning the model's data flow); jurisdictional / sovereignty issues and liability; unexplained / unexpected actions due to complex interactions and opacity; unethical / illegal decision-making (e.g. unequal demand reduction, market manipulation); human-machine interaction and overreliance / deskilling and supplier lock-in in a specialized market.

MIT Technology Review Insights (2021) describes that in oil and gas AI is becoming a critical cybersecurity defense for operational assets, since machine speed attacks can be detected by AI/ML solutions, despite the complexity of these environments. To respond to cyber risks businesses must adopt a risk-based approach by implementing AI enabled security tools and planning projects within a cybersecurity risk framework. This places AI as both operational optimizer and defensive layer in cyber-physical risk management.

According to Deloitte and USC Marshall Peter Arkley Institute for Risk Management (2024) analysis of annual risk factor disclosures of Standard & Poor's (S&P) 500 companies, AI is viewed as a "risk multiplier" for businesses. More than 60% of the companies examined, considered AI related risks to be material, and they disclosed AI related risks related to cybersecurity, competition/innovation, regulatory/legal exposure, intellectual property, ethics and reputation. AI is the most frequently mentioned in cybersecurity risk factors and over 40% of companies mentioned it, usually pointing to the increasingly advanced AI tools that attackers can use. Nearly 30% of firms reported difficulties adhering to changing AI laws and regulations; more than 15% mentioned difficulties with data protection and compliance and more than 17% mentioned changing AI related intellectual property laws, with disagreements over the status of AI generated works and concerns about infringement. The study also demonstrates that responsible AI has become a common risk category. Over 25% of respondents reported reputational risk from AI use, 15% reported ethical risks and 5% reported risks of biased, flawed or defective models or results harming society.

The European Union Artificial Intelligence Act (2024) is a governance regulatory document that categorizes AI into unacceptable, high-risk, limited risk and minimal risk categories and imposes many obligations on providers of high-risk systems. This risk based regulatory architecture has a direct impact on energy companies as AI deployers and buyers, especially considering the impact on critical infrastructure (supply of water, gas, heating and electricity), and in this case, AI is seen as a high-risk, and it is carefully regulated in this act. The act treatment of general-purpose AI (GPAI) is relevant as all GPAI model providers are required to provide technical documentation, instructions for use and a summary of training data content. For "Systemic risk" GPAI providers are required to conduct evaluations and adversarial testing, track/report serious incidents and ensure cybersecurity protections. For high risk systems there are particular requirements like: establish a risk management system for all the lifecycle of the system, have proper data governance, technical documentation, accurate record keeping that allows for proper risk identification, clear instructions for use and possibility for human oversight, appropriate levels of accuracy, robustness and cybersecurity as well as compliance ensured via a robust quality management system.

Methodology

This study employs systematic evidence mapping design, alongside structured content analysis to examine the application of AI in risk management within the energy sector. The approach is appropriate, as numerous pertinent AI implementations are recorded in diverse public sources (corporate disclosures, technology partner press releases, vendor deployment communications etc.) which offer qualitative descriptions but variable quantitative performance metrics and variate levels of disclosures. As a result, the study concentrates on identifying established adoption patterns, consistent risk control mechanism and intersectoral variations.

To create the data set, we first identified the top energy companies by revenues and then we looked for public disclosures or communication on the implementation and integration of AI in their processes with a focus on risk management. The database contains 50 units of analysis which is basically a company use case instance. Each record stores information about an AI application and how it is related to certain risk management stages and risk domain.

In the raw database each entry includes the company, country/region, sector, a detailed description of the AI use case, the risk management stages addressed, and the types of risk targeted. Because we observed that many AI systems go through more than one stage of the risk cycle, we modeled the risk stage as a multi-label attribute instead of a single category. Then we proceeded to normalize the raw text fields to parse and code them in a consistent way.

We utilized a reliable coding method to extract analytical variables that facilitate cross-sector comparisons. First, the steps of risk management were put into four groups: Identification, Analysis/Assessment, Prediction and Mitigation/Treatment. When stages were clearly defined, they were kept, when not, the narrative description was interpreted (for example "defect detection", "inspection" and "anomaly flagged" meant identification; "risk scoring" and "prioritization" meant analysis; "forecast" meant prediction and "remediation" or "preventive actions" meant mitigation).

Second, each record was assigned to one main AI capability class. Some of the capability classifications were: time-series predictive maintenance / anomaly detection, computer vision inspection, robotics and autonomy, digital twins and simulation, generative AI and neuro linguistic programming (NLP), forecasting and optimization, entity resolution and screening and cybersecurity analytics. For clarity and to avoid double counting, we prioritized explicit and detailed descriptions of mechanisms, rather than the general or ambiguous ones. Third, each record was linked to one main defined risk-control archetype, which was the main risk-control mechanism: condition-based reliability control (predictive maintenance (PdM) / asset performance management (APM)), inspection at scale (computer vision, drones, robots), operational decision support (control-room AI), digital twins for incident prevention, resilience forecasting and response optimization and enterprise risk screening/compliance/cyber controls. Because subsector field was too detailed, we grouped them into larger divisions for comparison.

Data processing was done using descriptive statistics, cross tabs and matrix analysis as well as dominance mapping to figure out what certain AI capabilities are most common in the risk lifecycles, via Excel files. We also wanted to examine the most common risk control regime per domain.

Results and discussions

In the heat map presented in Table 1, where 0 is the lowest point and 14 is the highest point, we can observe that there are two main ways that AI is used to control risks in energy. The first approach is focused on reliability and is mostly linked to predictive maintenance and anomaly detection over time. These solutions focus on the prediction and mitigation stages, which is part of a control chain that turns sensor information into early warnings or estimations of the possibility of failure and then into plans for maintenance and intervention. This pattern is common in places where rotating equipment is used and where high availability is important. In these situations, unscheduled downtime can have a big impact on operations and finances.

Table 1. Heat Map of AI Capabilities in Risk Stages (count of company use cases)

Risk Stage / AI Capability	Computer vision inspection	Digital twins / Simulation	Forecasting /Optimization	NLP / GenAI assistants	Mixed	Robotics / Remote inspection	Third-party screening / Entity-NLP	Time-series PdM / Anomaly detection
Identification	4	1	4	3	7	1	5	7
Analysis	1	0	1	4	2	1	3	2
Prediction	2	1	9	1	8	0	1	14
Mitigation	4	1	10	4	11	1	5	14

Source: authors' own research.

Figure 1 below highlights the importance of mitigation and treatment. AI seems to be a key tool used in this stage and rarely deployed as an analytics layer. While for risk analysis integration there is still room for improvement, AI systems seem to be more often part of decision and action pathways that link risk signals to operational actions. These responses can include prioritized remediation queues, automated maintenance workflow triggers, operator guidance or physical risk reduction via remote substitution. This conclusion is coherent with the control theoretical perspective that the value of risk management is contingent upon the reduction of detection to action cycle, rather than the enhancement of prediction in isolation.

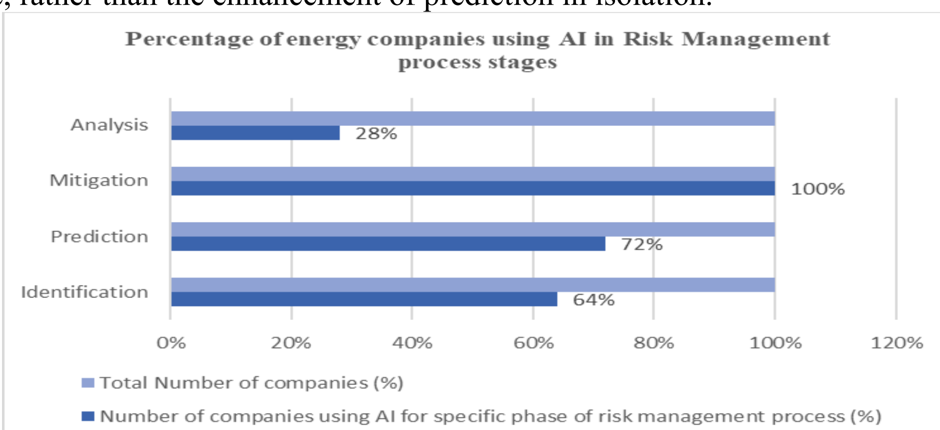

Figure 1. Utilization of AI capabilities in Risk Management process stages

Source: Authors' own research.

Figure 2 below shows a graph of subsector and dominating archetype typology and confirms that the AI risk fit depends on the domain. Due to sector's vulnerability to outages, fires and the necessity of prioritizing field interventions under regulatory reliability constraints, utilities and grid operators are primarily dominated by resilience forecasting / responses archetypes and inspections at scale. Because of the high cost of intervention, the safety criticality of barrier integrity and the value of early warning signals and virtual testing, upstream and offshore sectors are dominated by condition-based reliability control and digital twins. In the midstream there is a split between reliability control and inspection / threat detection, in line with integrity management and third-party damage exposure. Operational decision support archetype plays a more prominent role in refining and downstream contexts which are in line with anomalous situations management, process stability or compliance linked situations (like emissions and safety alerts). Nuclear sector is dominated by inspection at scale and remote substitution reflecting the importance of reducing exposures and the need for inspection evidence in safety critical situations.

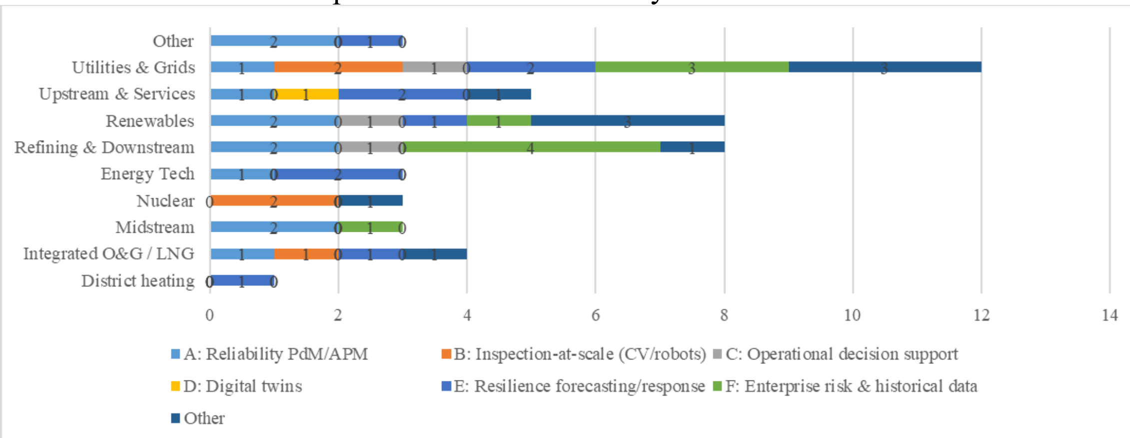

Figure 2. Dominating AI archetype by sub-sector (number of companies)

Source: Authors' own research.

Another area of examination was the AI proximity to control, which showed the maturity level. Findings show a slight movement from monitoring and detection to more integrated and sophisticated operational forms. The lower proximity is represented by monitoring/detection and advisory decision support, when AI supports human judgement but does not immediately initiate action. Workflow automation improves maturity by lowering bottleneck risk through standardized triage, fast decision and connecting AI results to intervention process (such as work order initiation and prioritized queues). The remote substitution introduces a unique maturity pathway: robots and autonomous inspections increase sensors frequency and coverage while lowering human exposure. The highest proximity category, closed loop or autonomous controls, is found in fewer cases, usually in areas where operating parameters can be defined, rigorous validation can be performed, and robust behavior can be designed.

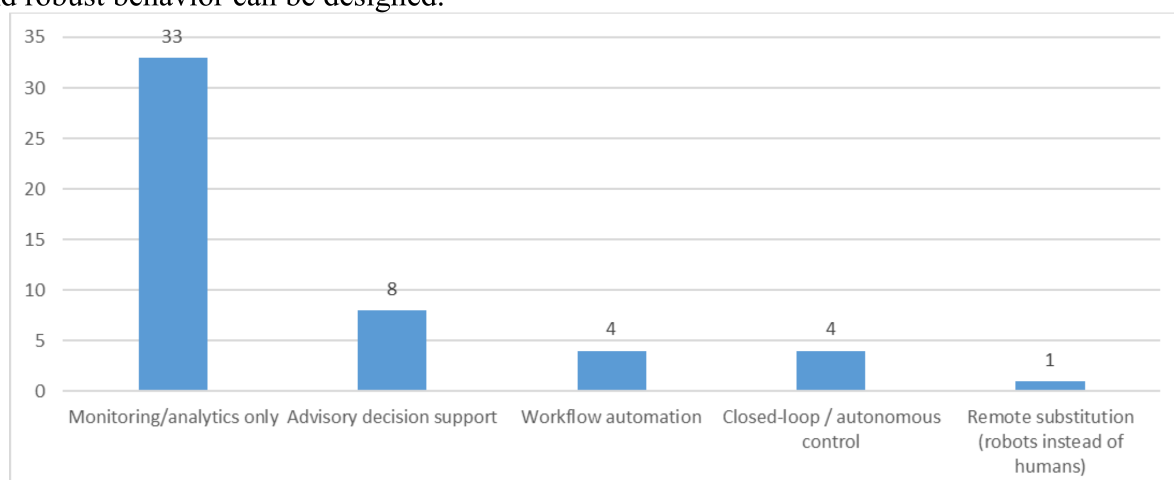

Figure 3. AI proximity to control (number of cases per control type)

Source: Authors' own research.

DOI: 10.2478/picbe-2026-0019, pp. 181-190, ISSN 2558-9652 |
Proceedings of the 20th International Conference on Business Excellence 2026

Conclusion

The database analysis demonstrates that companies primarily employ AI to mitigate risk by making quicker and more accurate decisions rather than merely analyzing the data.

Three primary categories of AI utilization are identified. Initially, numerous organizations implement predictive maintenance, which involves early detection of issues and the prediction of failures using sensor data. This approach enables the planning of repairs prior to the occurrence of malfunctions, thereby facilitating the prediction and mitigation of operational risk. Secondly, utilities, grid operators and nuclear-related organizations frequently employ computer vision, drones and robots to conduct large scale equipment inspections, identify defects, prioritize the severity and address the most hazardous ones first. This approach facilitates identification and mitigation, as well as minimizing workers' exposure to hazardous tasks. Third, AI is employed in the utilities and renewables sector to enhance system resilience and mitigate outage and market imbalance risks through forecasting and optimization (e.g. outage prediction, dispatch planning, demand forecasting).

The database also demonstrates the continued expansion of AI beyond physical assets to enterprise risk, including cybersecurity, compliance controls, and supplier / third party screening. In all sector seem to be a strong consensus that AI is most beneficial when it is linked to actual actions, reducing the time from problem discovery to problem resolution. However, most systems continue to require human intervention (monitoring and decision support), while fewer systems are approaching automatic controls (closed loop control, workflow automation or robotics replacing humans in hazards). This is because increased automation necessitates robust governance. In general, AI enhances risk management by facilitating the identification of issues at an earlier stage, expediting the response process, enabling experts to concentrate on the most critical issues and leveraging the knowledge of numerous assets throughout a fleet. However, it is essential to ensure that AI is backed by robust checks, including validation, model drift monitoring, audit trails, cybersecurity protections and secure backup options and to ensure existence of proper governance.

References

Wang, Q., Li, Y., & Li, R. (2025). *Integrating artificial intelligence in energy transition: A comprehensive review*. Energy Strategy Reviews, 57, 101600. https://doi.org/10.1016/j.esr.2024.101600.

Chen, H., Zhang, M., Zeng, J., & Wang, W. (2024). *Artificial intelligence and corporate risk-taking: Evidence from China.* China Journal of Accounting Research, 17(3), 100372. https://doi.org/10.1016/j.cjar.2024.100372.

Shobanke, M., Bhatt, M., & Shittu, E. (2025). *Advancements and future outlook of Artificial Intelligence in energy and climate change modeling*. Advances in Applied Energy, 17, 100211. https://doi.org/10.1016/j.adapen.2025.100211.

Khalil, M. A., Hadid, M., Padmanabhan, R., Elomri, A., & Kerbache, L. (2025). *An integrated Artificial Intelligence and optimization model for operational efficiency and risk reduction in Letter of Credit examination process.* Decision Analytics Journal, 14, 100552. https://doi.org/10.1016/j.dajour.2025.100552.

Milojević, N., & Redzepagic, S. (2021). *Prospects of Artificial intelligence and machine learning application in Banking Risk Management.* Journal of Central Banking Theory and Practice, 10(3), 41–57. https://doi.org/10.2478/jcbtp-2021-0023.

Gubareva, M., Shafiullah, M., & Teplova, T. (2024). *Cross-quantile risk assessment: The interplay of crude oil, artificial intelligence, clean tech, and other markets.* Energy Economics, 141, 108085. https://doi.org/10.1016/j.eneco.2024.108085.

Wong, L., Tan, G. W., Ooi, K., Lin, B., & Dwivedi, Y. K. (2022). *Artificial intelligence-driven risk management for enhancing supply chain agility: A deep-learning-based dual-stage PLS-SEM-ANN analysis.* International Journal of Production Research, 62(15), 5535–5555. https://doi.org/10.1080/00207543.2022.2063089.

Velev, D., & Zlateva, P. (2023). *Challenges of artificial intelligence application for disaster risk management.* International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, XLVIII-M-1–2023, 387–394. https://doi.org/10.5194/isprs-archives-xlviii-m-1-2023-387-2023.

Biolcheva, P. (2021). *The place of artificial intelligence in the risk management process*. SHS Web of Conferences, 120, 02013. https://doi.org/10.1051/shsconf/202112002013.

Rand, H. van Soest et al. (2024). The use of AI for improving energy security: Exploring the risks and opportunities of AI applications in the electricity system (RRA2907-1). RAND Europe

Rand, H. van Soest et al. (2024). The use of AI for improving energy security: Exploring the risks and opportunities of AI applications in the electricity system (RRA2907-1). RAND Europe

Rand, H. van Soest et al. (2024). The use of AI for improving energy security: Exploring the risks and opportunities of AI applications in the electricity system (RRA2907-1). RAND Europe

Rand, H. van Soest et al. (2024). *The use of AI for improving energy security: Exploring the risks and opportunities of AI applications in the electricity system* (RRA2907-1). RAND Europe. https://www.rand.org/pubs/research_reports/RRA2907-1.html.

Pantano, E., Marikyan, D., & Papagiannidis, S. (2023). *The dark side of artificial intelligence for industrial marketing management: Threats and risks of AI adoption*. Industrial Marketing Management, 116, A1–A3. https://doi.org/10.1016/j.indmarman.2023.11.008.

Future of Life Institute, (2024). *High-level summary of the AI Act.* https://artificialintelligenceact.eu/high-level-summary/.

KPMG. (2023). *Generative AI in energy, natural resources, and chemicals.* https://kpmg.com/us/en/articles/2023/kpmg-generative-ai-energy-natural-resources-chemicals.html.

MIT Technology Review. (2020). *Transforming the energy industry with AI.* https://www.technologyreview.com/

This paper was co-financed by The Bucharest University of Economic Studies during the PhD program.