AI and Cyber Threat Intelligence Management in the Energy Sector

Jyri Rajamäki, Ilkka Tikanmäki, Ronald Knowlton and Sonja Korhonen
Laurea University of Applied Sciences, Espoo, Finland

Jyri.rajamaki@laurea.fi

Abstract: Integrating artificial intelligence (AI) and cyber threat intelligence (CTI) into the energy sector has revolutionised the management of electrical systems and cybersecurity. This work-in-progress paper explores the current state and prospects of AI and CTI in the European energy sector, presenting a management model to ensure the ethical, transparent, and responsible use of AI within the DYNAMO project. The model leverages the ALTAI framework and the Z-Inspection® method, adhering to the requirements of the GDPR and the EU AI Act. AI is emerging as a key technology in managing electrical systems, optimising energy flow, and enhancing grid stability and operational efficiency. Examples include Siemens Spectrum Power and Schneider Electric's EcoStruxure. AI also aids in predicting electricity demand and renewable energy production, improving resource management and reducing waste. The EU AI Act classifies AI systems in the energy sector as high-risk, requiring stringent data protection, transparency, and human oversight. The ALTAI framework emphasises seven core principles: human agency, technical robustness, privacy, transparency, diversity, societal well-being, and accountability. The DYNAMO project aims to create a technical solution for small and medium-sized critical infrastructure companies to share CTI and support business continuity management. It uses the ECHO Early Warning System (E-EWS) for cyber threat information exchange. The AI governance model includes policies, processes, and technical frameworks to ensure AI systems remain ethical, secure, and responsible. Key components include encryption for secure data transfer, role-based access controls, integration of GDPR and EU AI Act requirements, and an adaptive framework with training modules and real-time feedback loops. Results indicate compliance with GDPR and EU AI Act requirements, effective response to new cyber threats, and high user satisfaction. This research underscores the importance of adaptability and regulatory compliance in AI governance frameworks. Future work includes real-world testing, iterative refinement, and broader stakeholder collaboration to further develop and validate the proposed model.

Keywords: AI governance, ALTAI, DYNAMO project, EU AI Act, Z-Inspection®

1. Introduction

Integrating AI into the energy sector and cybersecurity has revolutionised the management of electrical systems and cyber threat intelligence. The use of AI in cybersecurity, particularly in CTI, has introduced complex regulatory and operational challenges. Some of the more impactful challenges are balancing data privacy, security, and adaptability while ensuring compliance with frameworks such as the GDPR and the EU AI Act. On the other hand, the EU regulation aims to ensure the efficiency, competitiveness, and sustainability of the energy markets (European Parliament, 2024a). According to the AI Act (EU 2024/1689), the use of AI in energy sector systems is defined as high-risk (European Parliament, 2024b). These systems are subject to strict requirements for data protection, transparency, and human oversight. The Act requires surveillance for the use of AI and influences also influences organisations outside the Union borders (Heymann et al., 2023). However, the practical requirements for ensuring the safe use of AI are still lacking (Niet, 2022).

2. Research Methodology

This work-in-progress paper applies the Design Science Research Methodology (DSRM) (Hevner & Chatterjee, 2010). The first activity, *problem identification and motivation*, involves clearly defining the research problem and its significance, such as the challenges in managing AI and cybersecurity in the energy sector, identified in Work Package 2 "End-user & System Requirements" of the DYNAMO (2025) project. The second activity, *defining the objectives for a solution,* sets goals for the research, which in this paper is ensuring the reliability, security, and ethicality of AI systems.

This paper focuses on the third activity, *design and development*, where the artifact “the integration of the ALTAI framework and the Z-Inspection® method into AI system management” is created. The activities 4-7, *demonstration*, *evaluation*, and *communication* (Hevner & Chatterjee, 2010), are beyond the scope of this WIP paper.

3. AI in the Energy Sector

AI is emerging as a crucial technology for managing electrical systems, optimising energy flow, and enhancing grid stability and operational efficiency. Examples include Siemens Spectrum Power and Schneider Electric's EcoStruxure, which leverages AI for energy management and automation. AI also aids in forecasting electricity demand and renewable energy production, improving resource management and reducing waste (Rozite et al., 2023). AI’s ability to perform real-time analysis and decision-making makes it well-equipped to manage data-

driven environments such as power grids. AI systems can optimise the flow of energy, improving grid stability and operational efficiency. Examples of the use of AI in electrical systems include Siemens Spectrum Power and Schneider Electric's EcoStruxure. Siemens Spectrum Power leverages AI to monitor grid stability and optimise energy flows across electrical systems (Siemens AG, 2025). Similarly, (Schneider Electric, 2025) describes its EcoStruxure platform using AI for energy management and automation, driving efficiency across electrical networks.

One of the key contributions of AI to the energy sector is forecasting, particularly for electricity demand and renewable energy production (Khan et al., 2023). AI helps utilities manage resources, improving grid resilience and reducing energy waste. IBM's Environmental Intelligence Solution platform uses AI to provide climate insights, enabling businesses to anticipate disruptions, mitigate risks, and build sustainable operations (IBM, 2025). AI also plays a central role in business: by analysing large data sets, energy companies can better understand customer needs, enhance service offerings, and make data-driven decisions that increase operational efficiency and customer satisfaction (Heymann et al., 2023).

3.1 Cybersecurity and CTI

Integrating AI and CTI is vital for securing critical infrastructure such as power grids. AI enhances threat detection and defence mechanisms by identifying anomalies and automating routine cybersecurity tasks. In the long term, AI could provide proactive security anticipating and preventing attacks, although attackers may also use AI to develop more sophisticated threats.

The energy sector faces attacks from Advanced Persistent Threat (APT) actors, including spear phishing and ransomware campaigns. Effective CTI sharing requires reliable data, social trust, and overcoming fears of competition and reputation loss. Many EU energy operators lack a Security Operations Centre (SOC) for monitoring information technology (IT) and operational technology (OT) operations, indicating a need for improved capabilities.

Due to its criticality, the energy sector is a target of APT actors and faces attacks against Industrial Control Systems (ICS), as well as spear phishing and ransomware campaigns (Govea et al., 2024). In CTI, sharing reliable data and the management environment are emphasised, but sharing requires social trust between the parties (MITRE Corporation, 2012; Rajamäki, 2024). In addition to trust requirements, the fear of competition and losing reputation, as well as limited resources, hinder the CTI exchange within the sector (Paice and McKeown, 2023). Another issue is the current state of maturity within the available security products (Kalodanis et al., 2023) and their users. Approximately half of the EU energy operators do not use SOC for monitoring their IT/OT operations (ENISA, 2024). Therefore, it can be inferred that there remains work to do before the capabilities of SMEs enable effective CTI sharing.

3.2 Regulatory Considerations and Ethics

The AI Act (EU 2024/1689) classifies AI systems in the energy sector as high-risk, requiring rigorous data protection, transparency, and human oversight. To ensure the safe use of AI, it is essential to comply with these regulatory requirements and address the practical challenges associated with their implementation.

The Z-Inspection® methodology uses an interdisciplinary approach to identify ethical tensions and risks (Zicari et al., 2021). Z-Inspection® process evaluates the reliability of AI systems in practice. It is based on applied ethics and aims to ensure that AI systems are ethical, technically reliable, and suitable for the organisation. This process can help identify and manage ethical and technical risks associated with the use of AI in cybersecurity. For example, in the energy sector and the DYNAMO project, Z-Inspection® can help assess how well AI systems detect and respond to cyber threats, ensuring that the systems operate transparently and responsibly. Additionally, Z-Inspection® can help ensure that systems comply with the EU AI regulation and GDPR and provide feedback and recommendations for system improvements.

ALTAI (Assessment List for Trustworthy Artificial Intelligence) is a tool developed by the European Commission's High-Level Expert Group to help organisations assess the reliability of their AI systems. ALTAI focuses on seven principles: human agency, technical reliability, privacy, transparency, diversity, societal well-being, and accountability. The ALTAI framework can help ensure that AI systems comply with regulatory requirements, such as GDPR and the EU AI regulation, and that they are safe and ethical to use in cybersecurity. In the DYNAMO project, the ALTAI framework can guide the development and use of AI systems and provide recommendations and guidelines for adapting and improving the systems.

4. Proposed Ethical AI Governance Process for the Energy Sector

By integrating the Z-Inspection® (Zicari, et al., 2021) process and the ALTAI framework into energy sector management, a comprehensive governance model can be created that ensures the ethicality, safety, and accountability of AI systems. This can include the assessment of ethical and technical risks, ensuring regulatory compliance, and continuous improvement and adaptation through training modules and real-time feedback loops.

Table 1 presents the proposed framework for ethical AI governance in the energy sector. It has been developed by benchmarking the SHAPES project's ethical evaluation with the ALTAI tool (Rajamäki et al., 2023) and the pilot project "Responsible use of AI '' in cooperation with the Province of Friesland, Rijks ICT Gilde- part of the Ministry of the Interior and Kingdom Relations (BZK), applying Z-Inspection® Initiative (Boonstra et al., 2024).

Table 1: Ethical AI governance framework

Step	Description
Define the scope and objectives of the assessment.	*Clear scope:* Clearly define what aspects of the energy sector will be assessed, such as the management of electrical systems and cybersecurity measures. This helps focus on essential questions and avoid the assessment expanding too much. *Objectives:* Define the objectives of the assessment, such as ensuring the reliability, security, and ethicality of AI systems used in managing energy flow and grid stability.
Assemble a multidisciplinary assessment team.	*Experts*: Assemble a team that includes technical experts in AI and energy systems, ethical experts, cybersecurity experts, and possibly legal experts to ensure compliance with regulations like GDPR and the EU AI Act. *Common language:* Ensure that the team has a common language and understanding of the assessment's objectives and methods to facilitate effective communication and collaboration.
Use a structured assessment method (z-inspection or the ALTAI tool).	*Z-Inspection® process:* Utilize the Z-Inspection® process, which includes three phases: preparation, assessment, and resolution. This process helps identify and address ethical issues and tensions specific to the energy sector. *ALTAI process*: Utilize the checklists and concrete steps provided by the ALTAI tool to conduct the assessment, ensuring that all relevant aspects are covered systematically.
Evaluate technical aspects.	*Technical reliability:* Assess the technical reliability of the AI system, including data handling, labelling, system architecture, and robustness. This ensures that the AI system can effectively manage electrical systems and optimise energy flow. *Cybersecurity*: Ensure that the AI system meets cybersecurity requirements and has appropriate protection mechanisms to safeguard against cyber threats.
Evaluate ethical aspects.	*Human rights:* Assess how the AI system impacts fundamental rights, such as privacy, data protection, and good governance. This includes ensuring that the AI system does not infringe on the rights of individuals and communities. *Ethical principles:* Apply the ALTAI tool for trustworthy AI, focusing on principles such as respect for human autonomy, prevention of harm, fairness, and explicability.
Engage stakeholders.	*Users and decision-makers:* Engage the system's users and decision-makers in the assessment process. This helps ensure that their views and concerns are taken into account, leading to more effective and accepted AI solutions. *Transparency*: Ensure that the assessment results and recommendations are open and accessible to all stakeholders, fostering trust and collaboration.
Continuous monitoring and improvement.	*Monitoring*: Continuously monitor the use and impact of the AI system in the energy sector. Make necessary corrections and improvements to the system's operation and ethical aspects to maintain high standards. *Feedback*: Continuously collect feedback from users and stakeholders about the system's operation and ethicality. This helps identify areas for improvement and ensures the AI system remains effective and trustworthy.

By following these steps, the integration of AI and cyber threat intelligence into the energy sector can be managed effectively, ensuring that AI systems are reliable, secure, ethical, and respectful of fundamental rights.

5. Discussion and Conclusions

This work-in-progress paper's result is the concept of an ethical AI governance model, which provides a comprehensive approach to managing AI and cyber threat intelligence in the energy sector. The model

emphasizes ethicality, security, and regulatory compliance. Developing the model and achieving its full potential requires continuous testing, refinement, and collaboration with stakeholders.

The proposed governance model addresses the dual objectives of regulatory compliance and operational adaptability within the DYNAMO project, and it is easily extendable from the energy sector to other critical areas. By aligning AI governance with GDPR and the EU AI Act, this model provides a blueprint for secure and resilient CTI systems in cybersecurity. The integration of the ALTAI framework and Z-Inspection® method ensures that AI systems are ethical, transparent, and responsible, meeting stringent data protection and human oversight requirements.

The ethical AI governance model successfully enhances secure information sharing, compliance with regulatory standards, and user satisfaction. The adaptive framework, which includes encryption for secure data transfer, role-based access controls, and real-time feedback loops, demonstrates the importance of continuous monitoring and improvement in maintaining high standards of AI governance.

Future work involves DSRM's activities 4-7, such as real-world testing, iterative refinement, and broader stakeholder collaboration to further develop and validate the proposed model. Expanding the scope to include additional feedback mechanisms and scaling the model for broader applications will be crucial steps in ensuring its effectiveness and reliability.

Acknowledgements

Acknowledgment is paid to the DYNAMO Project, funded by the European Union under grant agreement no. 101069601. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Ethics declaration: Ethical clearance was not required for the research.

AI declaration: In section 3, the analysis of the articles by Rajamäki et al. (2023) and Boonstra et al. (2024) utilized artificial intelligence. The paper's spelling was verified using the artificial intelligence tool.

References

Boonstra, M., et al, 2024. Lessons Learned in Performing a Trustworthy AI and Fundamental Rights Assessment. https://doi.org/10.48550/arXiv.2404.14366

DYNAMO, 2025 Home. [online] https://horizon-dynamo.eu/

ENISA, 2024. Cyber Europe tests the EU Cyber Preparedness in the Energy Sector [WWW Document]. URL https://www.enisa.europa.eu/news/cyber-europe-tests-the-eu-cyber-preparedness-in-the-energy-sector (accessed 1.9.25).

European Parliament, 2024a. Energy policy: general principles [WWW Document]. URL https://www.europarl.europa.eu/factsheets/en/sheet/68/energy-policy-general-principles (accessed 1.9.25).

European Parliament, 2024b. Regulation - EU - 2024/1689 - EN - EUR-Lex (Regulation No. 2024/1689). European Union.

Govea, J., Gaibor-Naranjo, W., Villegas-Ch, W., 2024. Transforming Cybersecurity into Critical Energy Infrastructure: A Study on the Effectiveness of Artificial Intelligence. Systems 12, 165. https://doi.org/10.3390/systems12050165

Hevner, A. & Chatterjee, S., 2010. Design research in information systems: theory and practice. New York: Springer Science and Business Media.

Heymann, F., Parginos, K., Bessa, R.J., Galus, M., 2023. Operating AI systems in the electricity sector under European's AI Act – Insights on compliance costs, profitability frontiers and extraterritorial effects. Energy Reports 10, 4538–4555. https://doi.org/10.1016/j.egyr.2023.11.020

IBM, 2025. IBM Environmental Intelligence solutions [WWW Document]. Solutions. URL https://www.ibm.com/products/environmental-intelligence/solutions (accessed 1.9.25).

Kalodanis, K., Rizomiliotis, P., Anagnostopoulos, D., 2023. European Artificial Intelligence Act: an AI security approach. Information & Computer Security 32, 265–281. https://doi.org/10.1108/ICS-10-2022-0165

Khan, S.U., Khan, N., Ullah, F.U.M., Kim, M.J., Lee, M.Y., Baik, S.W., 2023. Towards intelligent building energy management: AI-based framework for power consumption and generation forecasting. Energy and Buildings 279. https://doi.org/10.1016/j.enbuild.2022.112705

MITRE Corporation, 2012. Cyber Information-Sharing Models: An Overview.

Niet, I., 2022. Between vision and practice: lack of alignment between AI strategies and energy regulations in the Dutch electricity sector. Discov Artif Intell 2. https://doi.org/10.1007/s44163-022-00040-6

Paice, A., McKeown, S., 2023. Practical Cyber Threat Intelligence in the UK Energy Sector, in: Onwubiko, C., Rosati, P., Rege, A., Erola, A., Bellekens, X., Hindy, H., Jaatun, M.G. (Eds.), Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media. Springer Nature, Singapore, pp. 3–23. https://doi.org/10.1007/978-981-19-6414-5_1

Rajamäki, J., 2024. Trust Environment for Cyber-Physical Systems: The DYNAMO Approach. International Journal on Applied Physics and Engineering 3, 1–10. https://doi.org/10.37394/232030.2024.3.1

Rajamäki, J., Gioulekas, F., Rocha, P.A.L., Garcia, X. del T., Ofem, P., Tyni, J., 2023. ALTAI Tool for Assessing AI-Based Technologies: Lessons Learned and Recommendations from SHAPES Pilots. Healthcare 11, 1454. https://doi.org/10.3390/healthcare11101454

Rozite, V., Miller, J., Oh, S., 2023. Why AI and energy are the new power couple [WWW Document]. Why AI and energy are the new power couple. URL https://www.iea.org/commentaries/why-ai-and-energy-are-the-new-power-couple (accessed 1.9.25).

Schneider Electric, 2025. EcoStruxure Platform [WWW Document]. EcoStruxure Platform. URL https://www.se.com/ww/en/work/campaign/innovation/platform.jsp (accessed 1.9.25).

Siemens AG, 2025. Grid Management Solutions with Spectrum Power [WWW Document]. siemens.com Global Website. URL https://www.siemens.com/global/en/products/energy/grid-software/operation/grid-control.html (accessed 1.9.25).

Zicari, R., Brodersen, J., Brusseau, J., Düdder, B., Eichhorn, T., Ivanov, T., Kararigas, G., Kringen, P., McCullough, M., Moslein, F., Mushtaq, N., Roig, G., Stuertz, N., Tolle, K., Tithi, J.J., Halem, I., Westerlund, M., 2021. Z-Inspection®: A Process to Assess Trustworthy AI. IEEE Transactions on Technology and Society 1, 16. https://doi.org/10.1109/TTS.2021.3066209