Compliance by Design for Cyber-Physical Energy Systems: The Role of Model-Based Systems Engineering in Complying with the EU AI Act

Dominik Vereno[a], Katharina Polanec and Christian Neureiter[b]
Josef Ressel Centre for Dependable System-of-Systems Engineering, Salzburg University of Applied Sciences,
Urstein Süd 1, 5412 Puch/Salzurg, Austria
fi

Keywords: Model-Driven Engineering, Domain-Specific Language, Risk Management, High-Risk AI Applications, Regulatory Compliance, Smart Grid.

Abstract: In the evolving landscape of intelligent power grids, artificial intelligence (AI) plays a crucial role, yet its integration into critical infrastructure poses significant risks. The new EU AI Act, regulating such high-risk applications, introduces stringent requirements such as risk management and data governance. This study aims to harness the potential of model-based systems engineering (MBSE) for enabling *compliance by design* in smart grids, ensuring adherence to regulation from early development stages. Through a detailed analysis of the AI Act's seven requirement for high-risk applications, the paper aligns them with established MBSE practices. The findings reveal MBSE as an effective tool for ensuring compliance, leading to three strategic recommendations: integrating mature disciplines into holistic MBSE approaches, establishing a broadly accepted AI modeling formalism, and creating a standardized model-based compliance assessment process. In conclusion, MBSE is a key enabler for creating dependable and safe AI applications, offering a positive outlook for future smart grid developments that are innovative yet compliant by design.

1 INTRODUCTION

The transition towards smart grids marks a pivotal development in modern electricity infrastructure, addressing challenges like integrating renewable energy and moving to electric transport (Farhangi, 2010). Artificial intelligence (AI) plays a crucial role in meeting these challenges and harnessing their potential to improve grid efficiency and stability through applications such as power-flow optimization, load management, fault detection, and information security (Ali and Choi, 2020). However, implementing data-driven decision-making in critical infrastructure necessitates strict adherence with regulatory frameworks.

The European Union‘s new regulation for harmonized rules on AI (AI Act) (European Commission, 2021) is a major regulatory milestone, with potential global implications. It categorizes AI applications based on risk levels, ranging from minimal to unacceptable. High-risk applications, which include those used in power grid operations, must adhere to seven stringent requirements covering aspects like risk management, data governance, and transparency. Navigating these regulations for complex grid applications poses significant challenges.

In navigating the complexities of cyber-physical systems of systems, model-based systems engineering (MBSE) emerged as a vital tool. At its core is the formalized application of digital models that supports various engineering activities ”beginning in the conceptual design phase and continuing throughout development and later life cycle phases” (INCOSE, 2007). MBSE is inherently suited to dealing with complexity via abstraction and separation of concerns (Neureiter et al., 2020). It further facilitates traceability throughout various modeling artifacts, such as components, requirements, and test cases.

The energy sector has been adopting MBSE approaches for over a decade (Lopes et al., 2011). A key development in this field is the Smart Grid Architecture Model (SGAM) (Smart Grid Coordination Group, 2012), which has inspired various standards-aligned, model-based engineering methods (Uslar et al., 2019). The SGAM Toolbox is a prominent example, focusing on high-level interdisciplinary modeling of energy use cases (Neureiter et al., 2016b). Such a holistic model-based approach is required to deal with the interdisciplinarity and complexity of

[a] https://orcid.org/0000-0002-7930-6744
[b] https://orcid.org/0000-0001-7509-7597

Vereno, D., Polanec, K. and Neureiter, C.
Compliance by Design for Cyber-Physical Energy Systems: The Role of Model-Based Systems Engineering in Complying with the EU AI Act.
DOI: 10.5220/0012623000003645
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 12th International Conference on Model-Based Software and Systems Engineering (MODELSWARD 2024)*, pages 365-370
ISBN: 978-989-758-682-8; ISSN: 2184-4348

smart grids. MBSE fosters a unified model instead of a disparate set of documents, bringing together diverse stakeholders. MBSE is therefore uniquely positioned to ensure compliance for AI applications in power grids.

This paper explores how the inherent benefits of MBSE can be leveraged to facilitate compliant AI applications in cyber-physical energy system. We focus on embedding compliance from the initial engineering stages, striving for *compliance by design*. There are two main research objectives and contributions:

1. Analyzing MBSE's potential in helping to meet the seven high-risk AI requirements, focusing on its benefits and existing MBSE efforts that could aid compliance.
2. Recommending essential areas for further research and consolidation, directed at researchers, practitioners, and regulatory authorities.

This research seeks to spotlight the intersection of MBSE and AI, emphasizing the significant role of MBSE in devising AI applications that are not only innovative but also compliant and safe. Our goal is to inspire progress in this promising field, with the ultimate objective of developing safe, reliable, and efficient energy systems for the future.

2 MBSE‘s ROLE IN ENSURING AI ACT COMPLIANCE

For high-risk applications, the AI Act lays out seven requirements. This chapter delineates each requirement and evaluates the role of MBSE in fulfilling it. We aim to assess the impact of MBSE, highlight existing work, and identify areas for further research. Table 1 outlines MBSE‘s impact on each requirement, using a scale from *Ancilliary (1)* to *Fundamental (4)*, to illustrate its potential in ensuring compliance.

2.1 Risk Management System

The AI Act mandates a continuous and iterative process for identifying, analyzing, and evaluating risks associated with AI systems. It involves implementing measures for risk reduction, including design considerations, control measures, and providing adequate user information.

With electricity infrastructure, risks range from minor disruptions to catastrophic failures that can threaten property and life. Risk management is thus critical in smart grids and is a well-established discipline across many domains. MBSE has emerged as an effective approach for risk management, offering comprehensive system models that capture complex interconnections and interdependencies. Relevant works in this area include the integration of failure mode and effects analysis (FMEA) into MBSE for early risk mitigation by (Hünecke et al., 2023) and the model-based assessment of security risks in smart grids by (Neureiter et al., 2016a); moreover, (Uludağ et al., 2023) present a comprehensive model-based risk management approach. MBSE‘s holistic perspective aids in early risk detection and ongoing management throughout a system's lifecycle, also facilitating effective communication of risk management strategies to stakeholders and regulatory bodies. However, advancements in this field require further maturation of model-based risk management approaches and the development of AI-specific risk management and modeling methods.

2.2 Data and Data Governance

For high-risk AI applications, providers must ensure data quality and robust data management practices. This entails using reliable datasets for training, validation, and testing. Data management also includes careful design choices in data collection and preparation, including annotation, cleaning, and bias examination, to guarantee datasets are relevant, representative, error-free, and complete.

This is particularly crucial as the volume and complexity of data in modern ICT-heavy power grids have increased dramatically.

With AI's growing role in critical operations, any data-related faults could have significant repercussions. MBSE provides an effective framework for creating detailed digital architecture models, crucial for modeling and managing data flows. Such models are likely a suitable basis for compliance assessment. For example, (Vereno et al., 2022) present an approach for model-based assessment of data quality, an essential compliance aspect. Moreover, the necessity to model data pipelines, processing steps, and AI-specific aspects like bias monitoring is evident. The RAMI 4.0 Toolbox (Binder et al., 2019), closely related to SGAM Toolbox, advances this approach further, offering a method for designing high-level information architecture to support AI integration (Binder et al., 2022). This work showcases the potential of MBSE in being a highly benefitial tool in ensuring compliant data governance.

Table 1: Potential impact of MBSE on fulfilling EU AI Act requirements for high-risk applications.

Article no.	Requirement name	Impact of MBSE
9	Risk management systems	Significant (3)
10	Data and data governance	Significant (3)
11	Technical documentation	Fundamental (4)
12	Record-keeping	Ancillary (1)
13	Transparency and provision of information to users	Ancillary (1)
14	Human oversight	Beneficial (2)
15	Accuracy, robustness, and cybersecurity	Beneficial (2)

2.3 Technical Documentation

AI regulation stipulates the need for comprehensive technical documentation, crucial for both regulatory compliance and maintaining AI solution integrity. This documentation should be prepared before market placement or service initiation. It must comprehensively capture the system's complexity, covering system descriptions, software architecture, and algorithms. The technical documentation allows authorities to thoroughly assess compliance, with specific elements detailed in Annex IV of the Act.

MBSE stands out as an inherently suitable methodology for this purpose, with its focus on creating comprehensive models that link heterogeneous aspects like requirements engineering, use case descriptions, and technical architecture. Despite MBSE‘s suitability, a challenge remains in the specific area of model-based engineering for AI. The current landscape, as reviewed by (Raedler et al., 2023), reveals a lack of a unified, widely accepted approach to AI-specific modeling. Establishing a standardized methodology in this area is necessary for integrating AI more effectively into MBSE frameworks. Such integration would not only streamline compliance efforts but also enhance the efficacy and reliability of the technical documentation process, thereby ensuring robust and compliant AI solutions.

2.4 Record-Keeping

High-risk AI systems must have capabilities for logging operations, ensuring traceability and accountability in their functioning. This is particularly crucial for monitoring performance and modifications.

Here, MBSE can offer support, although it is not a critical or necessary component. MBSE‘s strengths in modeling data flows can facilitate the setup and maintenance of logging and record-keeping mechanisms. However, the core principles of MBSE, which revolve around system architecture and design, do not directly align with the primary objectives of record-keeping. Essentially, while MBSE can contribute to a structured approach in managing data records, its role in this aspect of AI system compliance is more complementary than fundamental.

2.5 Transparency and Provision of Information to Users

Providers must establish transparency, providing users with clear, accurate information about the system's capabilities, performance, limitations, and intended use.

In addressing this requirement, MBSE can play a supportive role. While not critical for this requirement, MBSE can help by defining specific viewpoints in the system model that address user concerns, enhancing their understanding of the AI system‘s functionality. These viewpoints can detail the system's identity, capabilities, performance characteristics, limitations, and maintenance needs. The focus of MBSE in this context would be on creating clear, comprehensive views that facilitate user comprehension, thereby contributing to the overall transparency of high-risk AI systems.

2.6 Human Oversight

High-risk AI systems must be designed for effective human oversight. This involves integrating human–machine interface tools to enable human operators to intervene and override the system as needed, thereby minimizing risks to health, safety, or rights. These oversight measures, integral to the system's design, ensure that overseers can comprehend the AI's operations and outputs, stay alert to automation biases, and intervene effectively whenever necessary.

When operating the critical electricity infrastructure, it is crucial to ensure safe operation by having it overseen by human operators with the ability to step in when needed.

MBSE is particularly useful here, as it supports the design of AI systems by clearly outlining where and how human operators can interact and make decisions. This ensures that human oversight is an integral part of the system from the start.

Leveraging this potential requires incorporating the extensive work on human–machine interfaces and human-in-the-loop systems into established architecture frameworks. Thoroughly assessing the impact of human oversight and intervention further necessitates integrating human behavior models for validation and simulation, as explored in studies like those by (Ngo et al., 2022). The successful integration of these varied advancements is crucial for the multidisciplinary engineering of AI applications that are both safe and compliant, under effective human supervision.

2.7 Accuracy, Robustness, and Cybersecurity

The EU AI Act demands that high-risk AI systems must consistently exhibit high accuracy, robustness, and cybersecurity throughout their lifecycle. Providers must implement safeguards to ensure resilience against errors, faults, inconsistencies, and security threats. Additionally, AI systems that continue learning post-deployment must have mechanisms to mitigate biases resulting from feedback loops and protect against unauthorized alterations and attacks.

This is crucial in grid operations to ensure reliability and safety, preventing system failures and cybersecurity breaches which can have far-reaching consequences.

In this context, MBSE offers a valuable approach. It facilitates the integration of security assessments within the system design, particularly through tools like the SGAM Toolbox, as shown by (Neureiter et al., 2016a). However, integrating formalisms for accurately modeling and managing aspects such as system robustness and bias is an area that requires further development within MBSE. This is particularly important for detecting and mitigating biases, especially in systems that evolve or learn over time.

3 RECOMMENDATIONS

Our analyses revealed MBSE‘s varying degrees of impact across the seven requirements. While some aspects were specific to individual requirements, overarching trends emerged. Based on these findings, we propose three key recommendations to enable comprehensive MBSE for compliance by design. These recommendations are directed at academia, industry practitioners, and regulatory bodies.

3.1 Integrating Mature Disciplines with MBSE

Several areas addressed in the AI Act’s requirements are already mature discplines, including risk management, data governance, and human-in-the-loop systems (sections 2.1, 2.2, and 2.6). These fields are advanced and well studied. Our analyses have highlighted that it is critical to utilize them collectively, in order to not only comply with a subset of requirements, but all of them. Holistic MBSE approaches present ideal crucibles in which to bring the disparate disciplines together. Here, MBSE not only serves as a technical tool but as a comprehensive framework for an interdisciplinary compliance strategy.

There are two main challenges in this endeavor: First, for each discipline, (de-facto) standards for modeling have to be identified or established, requiring in-depth knowledge of the respective industry‘s best-practices and standardization. For example, the smart-grid community—with its great need for interdisciplinary cooperation—created the SGAM reference architecture framework; it also converged on a broadly used domain ontology, the Common Information Model (Uslar et al., 2012). Second, all such widely establish modeling approaches have to be properly formalized and harmonized with an established MBSE methodology. Such a harmonization has to take place on a semantic, syntactic, and tool-based level—requiring common ontologies, data-model standards, and programming interfaces. (Binder et al., 2021) found that in industrial engineering, simply introducing a theoretical concept—such as the RAMI 4.0 framework—is not enough. For practical application, it requires a formalized modeling approach and tool support.

3.2 Establishing a Broadly Accepted Modeling Formalism for AI

For most of the requirements, an approach for modeling AI aspects of a system are benefiticial. Particularly, the proper technical documentation (Section 2.3) proving compliance to various requirements would benefit significantly from such a modeling formalism. However, in the domain of model-driven AI engineering there is a noticeable lack of an established, widely-accepted methodology; rather, the field is characterized by a variety of disparate appraoches (Raedler et al., 2023). The lack of standardization not only hinders compliance efforts but also affects the overall quality and robustness of AI systems. This situation underscores the urgent need for the community to converge on a small set of standardized for-

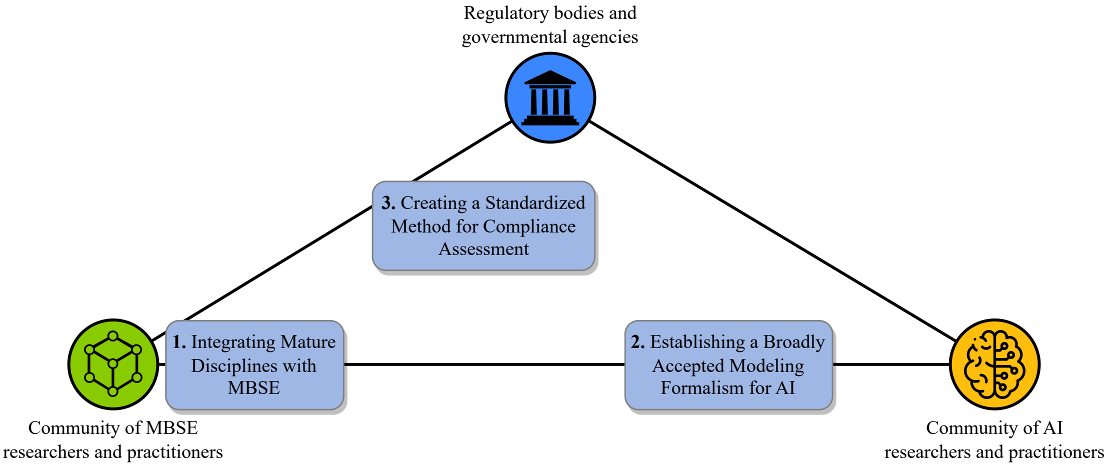
Regulatory bodies and governmental agencies
3. Creating a Standardized Method for Compliance Assessment
1. Integrating Mature Disciplines with MBSE
2. Establishing a Broadly Accepted Modeling Formalism for AI
Community of MBSE researchers and practitioners
Community of AI researchers and practitioners

Figure 1: Recommendations addressing MBSE and AI communities, and regulatory bodies.

malisms for AI description, which would then be integrated into broader MBSE methodologies. These formalisms should include aspects of explainable AI to ensure transparency and accountability in AI system design. Such consolidation would facilitate the detailed description of AI models, including aspects like hyper-parameterization, optimization goals, performance metrics, and bias monitoring, making it a pivotal step towards a more unified and effective approach to AI system design and assessment.

3.3 Creating a Standardized Method for Compliance Assessment

Looking into the potential impact of MBSE for assuring compliance has shown that there is a variety of approachs for using models to assess various system characteristics—e.g. risk, cybersecurity, and data quality. There is great potential in using comprehensive models to assess compliance. On the one hand, it enables compliance by design from the earliest stages of application development. On the other hand, it allows verification post-implementation, which is essential for regulatory agencies in charge of assessing adherence to the AI Act. Therefore, a standardized method for assessing compliance based on a model-based technical documentation is needed, including processes, guidelines, and tools. This necessitates collaborative efforts between academia, industry, and government to establish a clear, structured compliance assessment process. Standardizing compliance assessment methods will streamline audits and improve transparency, aiding providers to meet regulatory standards and to avoid penalties. It further offers regulatory bodies an efficient tool for assessing compliance in a continuous and cost-effective way.

4 CONCLUSIONS

AI is a significant driver in the modernization of power grids. To use this technology in the European energy infrastructure, it must be compliant with the EU AI Acts requirements for high-risk AI applications. The paper explores how the promising MBSE paradigm can enable developing such applications in way that ensures compliance by design. Our analyses underline that MBSE's inherent strengths make it an ideal tool for meeting the AI Act's requirements, especially in technical documentation, risk management, and data governance. MBSE shows immense potential in some areas, while in others, it likely plays a more supportive rather than a fundamental role.

The study highlights the need for action from the MBSE community, AI researchers and practitioners, as well as regulatory bodies. First, it is crucial to integrate well-established and mature disciplines with MBSE for comprehensive development. Second, the AI community must converge on a broadly accepted AI modeling formalism. Finally, a joint effort is needed to establish a standardized method for model-based compliance assessment. In conclusion, MBSE stands out as a key enabler for developing innovative yet compliant high-risk AI applications in smart grids. However, realizing this potential requires collaborative and interdisciplinary efforts to align advanced engineering practices with regulatory standards.

ACKNOWLEDGEMENTS

The financial support by the Austrian Federal Ministry for Digital and Economic Affairs and the National Foundation for Research, Technology and Development and the Christian Doppler Research Association as well as the Federal State of Salzburg is gratefully acknowledged.

REFERENCES

Ali, S. S. and Choi, B. J. (2020). State-of-the-art artificial intelligence techniques for distributed smart grids: A review. *Electronics*, 9(6).

Binder, C., Neureiter, C., Lastro, G., Uslar, M., and Lieber, P. (2019). Towards a standards-based domain specific language for industry 4.0 architectures. In Bonjour, E., Krob, D., Palladino, L., and Stephan, F., editors, *Complex Systems Design & Management*, pages 44–55, Cham. Springer International Publishing.

Binder, C., Neureiter, C., and Lüder, A. (2022). Towards a domain-specific information architecture enabling the investigation and optimization of flexible production systems by utilizing artificial intelligence. *The International Journal of Advanced Manufacturing Technology*, 123(1–2):49–81.

Binder, C., Neureiter, C., and Lüder, A. (2021). Towards a domain-specific approach enabling tool-supported model-based systems engineering of complex industrial internet-of-things applications. *Systems*, 9(2).

European Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence.

Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine*, 8(1):18–28.

Hünecke, P., Binder, C., Hoffmann, D., Lüder, A., and Neureiter, C. (2023). Facilitating fmea investigation of industrial systems during basic engineering with rami 4.0. In *2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–7.

INCOSE (2007). Systems Engineering Vision 2020. Technical Report INCOSE-TP-2004-004-02, International Council on Systems Engineering.

Lopes, A., Lezama, R., and Pineda, R. (2011). Model based systems engineering for smart grids as systems of systems. *Procedia Computer Science*, 6:441–450. Complex adaptive sysytems.

Neureiter, C., Binder, C., and Lastro, G. (2020). Review on domain specific systems engineering. In *2020 IEEE International Symposium on Systems Engineering (ISSE)*, pages 1–8.

Neureiter, C., Eibl, G., Engel, D., Schlegel, S., and Uslar, M. (2016a). A concept for engineering smart grid security requirements based on sgam models. *Computer Science - Research and Development*, 31(1):65–71.

Neureiter, C., Uslar, M., Engel, D., and Lastro, G. (2016b). A standards-based approach for domain specific modelling of smart grid system architectures. In *2016 11th System of Systems Engineering Conference (SoSE)*, pages 1–6.

Ngo, S., DeAngelis, D., and Garcia, L. (2022). Modeling human-cyber interactions in safety-critical cyber-physical/industrial control systems. In *2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems (MASS)*, pages 716–717.

Raedler, S., Berardinelli, L., Winter, K., Rahimi, A., and Rinderle-Ma, S. (2023). Model-driven engineering for artificial intelligence – a systematic literature review.

Smart Grid Coordination Group (2012). Smart grid reference architecture. Technical report, CEN/CENELEC/ETSI, Brussels, Belgium.

Uludağ, Y., Evin, E., and Gürbüz, N. G. (2023). Integration of systems design and risk management through model-based systems development. *Systems Engineering*, 26(1):48–70.

Uslar, M., Rohjans, S., Neureiter, C., Pröstl Andrén, F., Velasquez, J., Steinbrink, C., Efthymiou, V., Migliavacca, G., Horsmanheimo, S., Brunner, H., and Strasser, T. I. (2019). Applying the smart grid architecture model for designing and validating system-of-systems in the power and energy domain: A european perspective. *Energies*, 12(2).

Uslar, M., Specht, M., Rohjans, S., Trefke, J., and Vasquez Gonzalez, J. M. (2012). *The Common Information Model CIM: IEC 61968/61970 and 62325 - A practical introduction to the CIM*. Springer Berlin Heidelberg.

Vereno, D., Polanec, K., and Neureiter, C. (2022). Evaluating and improving model-based assessment of contextual data quality in smart grids. In *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5.