

Simulative Analysis of Multi-Agent Systems in Energy Systems: Impact of Communication Networks

Malin Radtke^a and Emilie Frost^b

Distributed Artificial Intelligence, OFFIS - Institute for Information Technology, Oldenburg, Germany
{malin.radtke, emilie.frost}@offis.de

Keywords: Multi-Agent Systems, Simulative Analysis, Cyber-Physical Energy Systems, Communication Systems.

Abstract: This paper addresses the growing use of Multi-Agent Systems (MASs) in power systems, particularly within the context of Cyber-Physical Energy Systems (CPES). The reliance on Information and Communication Technologies (ICT) is critical for coordinating control and ensuring reliable information exchange. Disruptions in the ICT system can degrade overall system performance. Given the complexity of these systems, systematic testing and accurate simulation of MAS behavior under the influence of communication networks are essential to ensure stability and security of supply. The paper provides a structured perspective on how to analyze MASs performance under different communication conditions in CPES, offering recommendations based on literature. It serves as a guide to understanding the challenges posed by the integration of ICT into power systems, with guidelines that can be used and extended to evaluate and improve system performance.

1 INTRODUCTION

Multi-Agent Systems (MASs) have a wide range of applications in various domains, including smart grids, smart manufacturing, sensor networks, and intelligent transportation systems (Zhang et al., 2021). Extensive literature highlights the use of MASs in these fields, particularly in smart grids, where researchers are exploring their broad potential (Mahela et al., 2022).


As these applications evolve, the integration of Information and Communication Technology (ICT) into power systems is becoming increasingly critical. Traditional power systems, once reliant solely on physical infrastructure, are now increasingly integrated with ICT, encompassing advanced control, computing, and communication functions (Yohanandhan et al., 2020). This integration has led to the development of Cyber-Physical Energy Systems (CPES), which merge physical components of the power grid with cyber systems that monitor, control, and optimize the performance of the entire network (Hasanuz-zaman Shawon et al., 2019).


The reliance on ICT for coordinating control and information exchange among agents in CPES means that any disruption in communication networks can lead to significant system degradation (Zhou et al.,

2021). For instance, unexpected physical faults or cyber attacks can compromise the system's ability to maintain stability, efficiency, and security (Zhang et al., 2021). The complexity of these interactions highlights the need for systematic testing and modeling methods that can accurately simulate the behavior of MASs under various network conditions (Yohanandhan et al., 2020).

Given these challenges, it is crucial to conduct a thorough and systematic investigation of the complex interactions between MASs and the communication networks within CPES. This investigation should focus on understanding how communication networks influence the overall performance and reliability of MASs. Moreover, there is a growing need to develop robust strategies and architectures that can mitigate these risks and ensure the secure operation of CPES (Wang and Govindarasu, 2020a).

In this context, this position paper introduces a structured methodology for simulating and analyzing MASs in CPES, with an emphasis on how communication networks impact their performance and reliability. Rather than delivering definitive solutions, this paper offers a structured perspective on how such an analysis might be conducted. Specifically, the morphological box presented herein is not intended to be prescriptive, but rather serves as a theoretical guide based on current literature, reflecting one possible approach to tackling these complex issues.

^a  <https://orcid.org/0009-0009-9902-1744>

^b  <https://orcid.org/0000-0003-4791-2333>

By examining various parameters and scenarios that impact MAS performance, this paper seeks to provide a conceptual framework to understand and address the challenges posed by the integration of ICT in modern power systems.

In particular, the paper includes research on related work for analysis of MASs, as discussed in section 2. In section 3, selected literature is used to illustrate the basis for the proposed morphological box, which demonstrates key objectives and design decisions critical to such a simulative analysis. Finally, the implications of these findings are discussed and concluded in section 4.

2 RELATED WORK

In this section, we categorize and identify contributions relevant to the simulative analysis of MASs in CPES under the influence of communication networks. Additionally, we highlight limitations in existing related work, that provide a foundation for the more detailed analysis guidance.

Agent-Based Applications in CPES.

Hasanuzzaman Shawon et al. (2019) and Mahela et al. (2022) provide comprehensive reviews of agent-based applications in smart grids, focusing on MAS concepts, design, challenges, and technological frameworks. Agents are categorized based on their roles in energy management (e.g., pricing, scheduling) and on ensuring reliability and security (e.g., fault handling). However, they do not delve into how communication network issues impact system performance, particularly under fault conditions or cyber attacks. This paper builds on their insights by specifically addressing these gaps through the proposed simulative analysis guideline.

Safety and Security Analysis in MASs. Zhang et al. (2021) provide an in-depth survey on the safety and security of MASs, with a focus on fault estimation, detection, diagnosis, and fault-tolerant control. While this research offers a strong theoretical framework, its abstract nature limits practical applicability, particularly in energy systems. The focus is primarily on fault detection rather than simulative investigations that explore MAS behavior under real-world fault and attack scenarios. Yohanandhan et al. (2020) review various modeling and simulation methods related to cybersecurity in CPES. This includes a detailed overview of cyber attack types, such as Denial of Service (DoS), Malware, and Man-in-the-Middle attacks, and their potential

impacts on physical systems, including stability and economic factors. However, the review remains general, lacking specific guidelines or best practices for analyzing MASs under the influence of communication networks.

Research Gap. The reviewed literature provides valuable foundations for understanding MASs in CPES, safety and security concerns, and the role of ICT. However, there are notable gaps, particularly in the simulative analysis of MAS behavior under the influence of communication networks. Existing research tends to focus either on abstract, theoretical concepts or general cybersecurity in CPES without providing specific guidelines or practical approaches for investigating MASs in the context of energy systems. This position paper aims to fill these gaps by proposing a comprehensive guide for simulative analysis, addressing the key objectives and design decisions necessary for robust and reliable MAS operation in CPES.

3 SIMULATIVE ANALYSIS OF MAS

The analysis of MASs in CPES necessitates a comprehensive understanding of the role communication networks play in determining the performance and behavior of these agent systems. Communication networks, which serve as the critical infrastructure for data exchange between agents, can significantly impact system stability, reliability, and efficiency. To investigate these impacts, a simulative analysis offers a robust approach to assess how variations in communication conditions, such as latency, packet loss, or network failures, influence MAS performance.

This section presents a structured methodology for conducting a simulative analysis of MASs under the influence of communication networks in CPES. Drawing on insights from existing literature, the guidance is divided into several key areas:

- the definition of analysis objectives,
- the specification of system requirements and communication threats,
- and the design of the simulation study itself.

Using a morphological box (see Figure 1), we categorize critical parameters that affect MASs in CPES, providing a comprehensive guideline to systematically assess the interplay between MASs and communication networks. The aforementioned key areas and parameters are presented and detailed below, as shown in Figure 1.

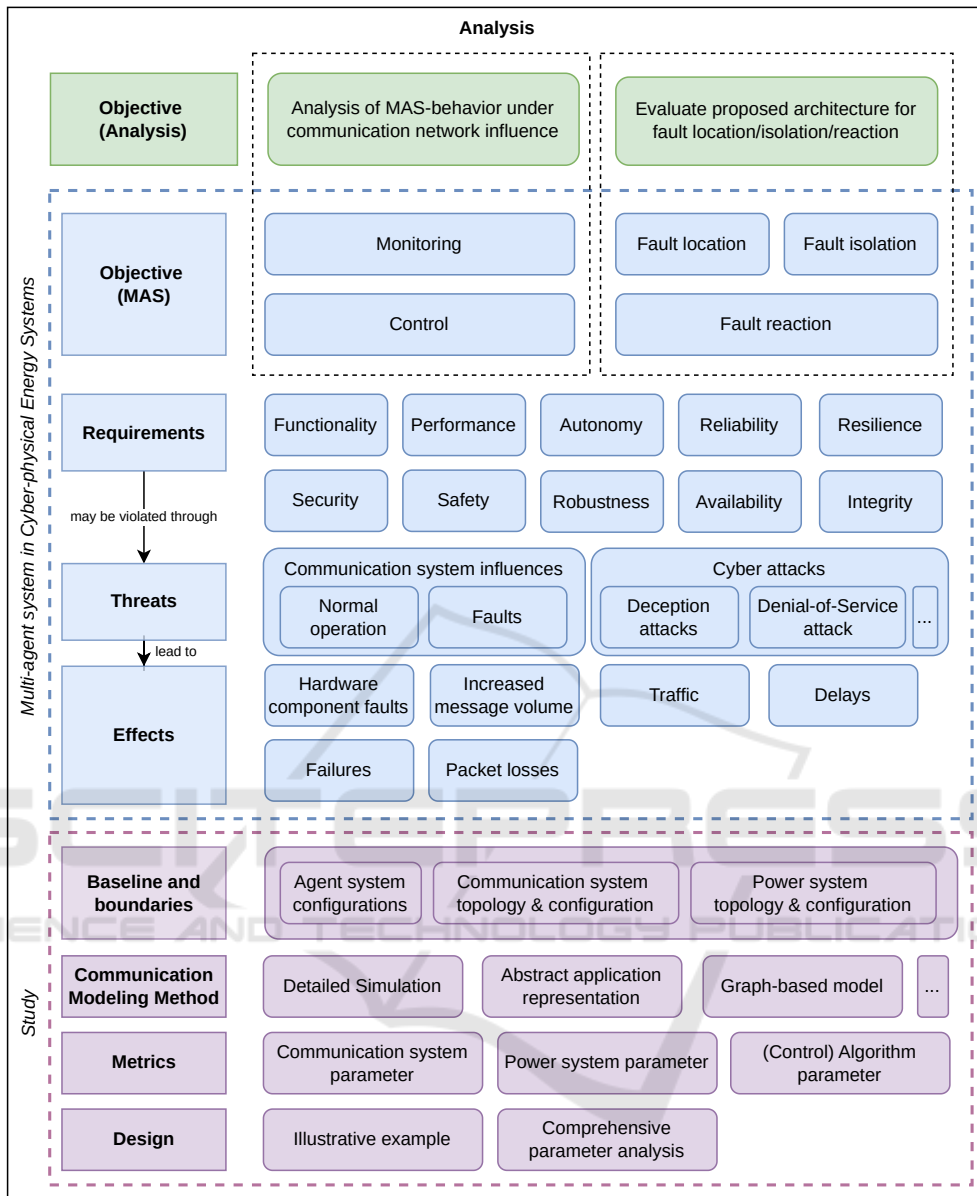


Figure 1: Overview of important parameters in the simulative analysis of MASs in CPES.

3.1 Analysis: Objective

The analysis objective addresses the purpose of conducting the simulative analysis itself. It defines what the analysis aims to achieve, such as understanding how communication network conditions affect MAS behavior or assessing the efficacy of fault-handling architectures.

One key objective when conducting a simulative analysis may be to *understand how MAS behavior and performance are influenced by different communication network conditions*. This process assists in the identification of potential vulnerabilities and the opti-

mization of the system. It includes investigating the impact of communication network performance metrics such as latency and packet drops, as well as failures or attacks on power system applications.

For example, Xiahou et al. (2021) studied the reliability of power systems under random delay attacks, while Radtke et al. (2023) investigated the influence of a realistic communication network on the power system applications redispatch and voltage control under varying communication network conditions. Secondly, the *evaluation of the proposed architectures for fault detection, isolation, and reaction* provides valuable insights into the effectiveness of MASs

in handling communication faults and cyber attacks. For instance, Wang and Govindarasu (2020a) evaluated their proposed anomaly detection mechanism, while Albarakati et al. (2023) demonstrated the efficacy of adaptive protection mechanisms. Other studies, such as the work of Ilyes et al. (2019), focused on frameworks to detect and reconfigure systems after cyber attacks and physical faults.

3.2 System: Objective

In contrast to the objective of analysis, the objective of the system focuses on the intended goals of the MAS within the context of the energy system. This subsection highlights the primary functions that the MAS is designed to perform, such as energy management or fault detection and reaction (Mahela et al., 2022), and emphasizes how these specific system objectives shape the focus of the analysis.

If the primary objective of the MAS is related to *monitoring and control* functions in the power grid (such as in Xiahou et al. (2021); Yang et al. (2020)), the analysis would usually focus primarily on understanding the MAS behavior under the influence of communication networks.

Conversely, when the objective of the agent system lies more in *fault location, isolation, and reaction* (such as in Albarakati et al. (2023); Ilyes et al. (2019); Abdelhamid et al. (2022)), the analysis shifts towards evaluating proposed architectures for handling communication faults and responding to cyber attacks. In this case, the focus is on testing the effectiveness of the agent's ability to detect, isolate, and recover from faults in communication networks in the analysis.

3.3 System: Requirements

In the context of energy systems, different requirements must be met by MASs. Depending on the objective in the development of the MAS and the application, these requirements differ. Many approaches consider *security* as a requirement for MASs. According to Hines et al. (2014), security in the context of power systems means that no component will cause the system to violate the operating limits. In the context of smart grids, security often refers to cyber security, as designing communication systems resistant to attempted cyber attacks. This is also done in the literature, as many approaches consider security of MASs against cyber attacks (Ilyes et al., 2019; Zhou et al., 2021; Wang and Govindarasu, 2020a; Choi et al., 2020) or faults (Abdelhamid et al., 2022). According to Hines et al. (2014), security is often associated with *robustness*, meaning that a secure system is ro-

bust against attacks or failures. Therefore, similar to security, robustness is also required for MASs. Albarakati et al. (2023) define robustness as the system's ability to cope with disturbances while maintaining functionality. Thus, approaches in the literature investigate the robustness of their MAS regarding faults and attacks, for example, to ensure that the system is robust under packet drops or time delays (Oest et al., 2021; Yang et al., 2020).

Additionally, *reliability* is considered a requirement for MASs, which can be defined as continuous delivery of a correct service (Sanislav et al., 2017). The actual service depends on the application of the MAS, as service availability, latency, duration of outages (Hines et al., 2014) or the delivery of electricity (Arghandeh et al., 2016). In the literature, reliability of MASs is considered regarding cyber attacks (Fang et al., 2017; Sanislav et al., 2017; Choi et al., 2020; Oest et al., 2021) or evaluated for distributed approaches (Kou et al., 2021). Similar to the previous metrics, *functionality* is a requirement for MASs (Zhu et al., 2019). Robust systems are maintaining functionality during disturbances (Arghandeh et al., 2016). However, the definition of functionality is also depending on the application and the system itself. The *performance* is often analyzed as a requirement for MASs, however, the interpretation depends on the use case. For different applications, different metrics are defined, such as solution quality (Oest et al., 2021). Furthermore, *resilience*, meaning the ability of a system to recover from a failure (Hines et al., 2014) is required in MASs (Wang and Govindarasu, 2020a). This includes for example service restoration (Abdelhamid et al., 2022). Other requirements are also possible, depending on the application and objective. These include for example *autonomy* (Sanislav et al., 2017; Oest et al., 2021), *safety* (Sanislav et al., 2017; Ilyes et al., 2019), *availability* (Fang et al., 2017; Kou et al., 2021) or *integrity* (Fang et al., 2017).

3.4 System: Threats

The aforementioned requirements that apply to MASs in energy systems may be violated through a variety of threats concerning the impact of the communication network on the system. These threats can be classified into two main categories: those that affect the system under normal operating conditions or in the event of technical faults, and those that are of a cyber attack nature.

In examining the *impact of communication networks under normal operational conditions*, it is possible to consider the integration of packet drops and packet delays in message dispatch (Yang et al., 2020),

as well as the evaluation of system behavior under the influence of different communication technologies (Oest et al., 2021). Furthermore, the influence of technical faults, such as communication link or base station failure, may also be analyzed (Abdelhamid et al., 2022; Oest et al., 2021).

Cyber attacks have recently been perceived as particularly threatening and therefore have also been analyzed regarding their impact on MASs. Fang et al. (2017) regard cyber attacks in general, while other authors focus on specific attacks, as deception attacks (Wang and Govindarasu, 2020a). Often investigated are DoS attacks, as the effects of such an attack can take many forms, such as system failures or overloads (Wang and Govindarasu, 2020a; Albarakati et al., 2023). Other attacks deal with false data being transferred via the system. As this also impacts a MAS, these types of attacks are extensively investigated in the scientific literature. Most of the time, false data injection attacks are considered in this case (Ilyes et al., 2019; Zhou et al., 2021; Choi et al., 2020) or man-in-the-middle attacks (Sanislav et al., 2017). Other approaches investigate false data or data manipulations in specific areas, such as alert manipulation attacks (Zhou et al., 2021) or configuration change attacks (Sanislav et al., 2017).

3.5 System: Effects

While some approaches investigate the threat itself, others focus on the effect of such threats. Different threats have different effects on the system. The investigated effects are *hardware component faults* due to attacks (Sanislav et al., 2017), *failures* (Wang and Govindarasu, 2020b), *increased message volume* (Frost et al., 2024), *traffic* (Radtke et al., 2023), *delays* or *packet losses* (Oest et al., 2021; Frost et al., 2020; Yang et al., 2020; Xu et al., 2021). Several of these effects are caused by multiple threats, such as failures or attacks, as failures of assets can be caused by environment or denial of service attacks.

3.6 Study: Baseline and Boundaries

Establishing the baseline and boundaries for the simulative analysis is a critical first step to accurately assess the behavior of MASs within CPES in a simulation study. This process involves defining the initial configuration of the system, agent behavior, characteristics of the communication network, and the topology of the power system. By setting a clear baseline, the analysis can systematically vary different parameters to assess the system performance under a range of conditions.

The baseline should include a *well-defined model of the MAS*, specifying the number and type of agents, and the specific objectives they are designed to achieve (e.g., fault detection, optimization, or control). For example, studies such as Sanislav et al. (2017) and Oest et al. (2021) include detailed configurations of agent systems and communication technologies, which serve as starting points for their analyses.

The *topology and configuration of the communication system* are also critical components of the baseline. This includes defining communication technologies and network architectures. Variations in communication conditions, such as the introduction of delays or failures, can then be explored based on this baseline configuration. For instance, Frost et al. (2024) assessed the influence of a wired communication network with ring and star topologies in three distinct scenarios: an ideal communication environment, an unimpaired scenario, and an attack situation.

Finally, the *power system topology and configuration* must be specified, including details about the physical grid model, such as the number of buses, feeders, and generators. The baseline might be based on real-world systems, such as the distribution feeder used in Albarakati et al. (2023) or standard models such as the IEEE 9-bus system (Ilyes et al., 2019).

By carefully defining the baseline and boundaries, the analysis can ensure that any variations introduced in the scenarios (whether related to the agent system, communication conditions, or power system configurations) are meaningfully compared against a consistent reference point. This approach facilitates a comprehensive understanding of how different parameters influence the overall performance and reliability of the MAS within CPES.

3.7 Study: Communication Modeling Method

An important aspect of simulative analysis is determining the method for communication modeling. Different approaches exist, each varying in complexity, accuracy, and suitability depending on the purpose of the analysis. The choice of method affects the level of detail that can be captured regarding the influence of communication networks on MASs in CPES.

One common approach is the *integration of Key Performance Indicators (KPIs)*. This method models basic communication parameters such as delays or packet losses using stochastic distributions, simulating network influence without detailed network behavior. While this approach is simpler and less computationally expensive, it may lack the realism re-

quired to model complex interactions. For instance, Xiahou et al. (2021) use this approach to integrate random delay attacks into their analysis, providing a general understanding of how such disruptions affect system performance.

A more comprehensive approach is a *detailed simulation* conducted using specialized communication network simulation frameworks. This method allows for modeling specific communication technologies, protocols, and phenomena like interference, providing a more accurate and realistic representation of network behavior. However, it comes with drawbacks, such as increased complexity, higher computational overhead, and potentially costly licenses for simulation tools. Studies like Wang and Govindarasu (2020a) and Oest et al. (2021) demonstrate this approach, leveraging detailed simulations to evaluate performance under varying network conditions.

Alternatively, the *abstract application representation* method focuses on the effects of the communication network on the messages exchanged by agents, without explicitly modeling the network itself. This approach simplifies the analysis by assuming certain conditions, such as attack probabilities or transmission errors, and analyzing their impact on system performance. This method is used in studies like Fang et al. (2017), where attack probabilities are assumed to study system behavior, and in Albarakati et al. (2023), which models cyber attacks in data transmission without detailed network modeling.

Some studies also use *graph-based models* to represent communication networks. In this method, nodes in the graph represent communication nodes (e.g., agents), and edges represent communication links, which may be weighted based on network properties such as bandwidth or latency. This approach provides a flexible way to analyze network topologies and their impact on communication. For example, Es-lami et al. (2022) and Yang et al. (2020) use graph-based models to represent and simulate network performance, particularly in scenarios involving packet drops or communication delays.

3.8 Study: Metrics

The selection of appropriate metrics is a critical component of study design, as it defines how the performance of the MAS under the influence of the communication network will be evaluated. These metrics should be aligned with the overall objectives of the analysis and tailored to the specific scenario under investigation. Typically, the metrics can be categorized based on their origin: communication system parameters, power system parameters, and MAS or control

algorithm performance.

The *parameters of the communication system* are crucial to assess how the network influences MAS performance. These metrics typically focus on network delays, latency, and message losses. For example, Xiahou et al. (2021) measure delay times to evaluate the effects of random delay attacks, while Oest et al. (2021) examine end-to-end latency in different communication technologies to assess overall communication performance.

The *parameters of the power system* provide insight into how the grid itself is affected by communication issues or cyber attacks. Metrics such as current levels, breaker status during disruptions, or power output of generators are often used to evaluate grid stability and resilience. Studies like Albarakati et al. (2023) measure breaker status during cyber attacks, while Yang et al. (2020) track the optimized power output of generators to assess system performance under various network conditions.

Agent system and control algorithm parameters are essential for evaluating how well the agents or control algorithms perform within the system (under the influence of the communication network). Metrics in this category might include fault location accuracy, failure rates, and optimization run-times. For instance, Wang and Govindarasu (2020a) evaluate anomaly detection performance, and Albarakati et al. (2023) measure fault location accuracy. Oest et al. (2021) focus on metrics like negotiation times and error rates for optimization tasks, while Ilyes et al. (2019) track system reliability and failure rates.

3.9 Study: Design

The design of the study is important for shaping the insights that can be derived from the simulative analysis. Two common approaches are illustrative case studies and comprehensive parameter analysis.

An *illustrative example or case study* is often used to showcase the behavior of the system under a specific set of conditions. These case studies are typically designed around predefined scenarios, such as cyber attacks, communication faults, or system failures, and are meant to provide qualitative insights into the system's performance in specific contexts. For example, Fang et al. (2017) explore five different attack scenarios, while Wang and Govindarasu (2020a) focus on a single attack scenario to evaluate the system's response. Similarly, Albarakati et al. (2023) present three different scenarios, and Zhou et al. (2021) evaluate different fault and attack types. These case studies offer targeted insights, but may not capture the full range of system behaviors.

In contrast, a *comprehensive parameter analysis* systematically explores how changes in key parameters affect system performance across a wider range of conditions. This approach involves running multiple simulations while varying parameters such as agent system size, network conditions, or disturbance intensity to capture a more holistic understanding of system dynamics. For instance, Kou et al. (2021) conduct an extensive analysis of reliability metrics, and Oest et al. (2021) investigate how different agent sizes and communication technologies impact system performance in various scenarios.

Both approaches have their advantages. Case studies are ideal for demonstrating the system response to specific conditions, while comprehensive parameter analysis allows for a more generalized understanding of system behavior under a range of disturbances. The choice between these approaches should be aligned with the objective of the analysis and the level of detail required for the analysis.

4 DISCUSSION AND CONCLUSION

A principal conclusion to be drawn from this guideline for simulative analysis is the necessity for MASs to be communication-aware. This implies that decision-making algorithms in energy systems should be constructed in a manner that enables them to function with incomplete or delayed information. The concrete definition of requirements for the system allows the identification of potential impairments resulting from the influence of the simulated communication network. This enables analyzing the system's behavior under adverse conditions (e.g., due to cyber attacks) and the implementation of suitable security mechanisms. The use of appropriate detection mechanisms allows for the mitigation of faults and attacks before system stability is compromised. Investigations into the scalability of such systems also benefit from the simulation analysis proposed, as these studies highlight the importance of considering potential (communication) bottlenecks in large systems. Furthermore, simulative analysis of MASs under influences of the communication network assists in selecting appropriate communication technologies and protocols by evaluating and comparing diverse options.

Although the guideline provides a solid foundation, it may not cover all possible scenarios or system configurations and must be applied to real-world use cases. Users are encouraged to expand and adapt the guideline based on their own needs, incorporating additional parameters, or exploring new technologies,

such as emerging cyber threats and communication technologies.

In summary, this paper serves as a guide for understanding and addressing the challenges posed by the interconnections of ICT and power system, and proposes a structured approach to evaluating the performance of MASs under communication conditions in CPES in a simulative analysis. Recommendations are given on what aspects should be considered in such an analysis, based on the current literature. Future work may include examples of the practical application of these guidelines to new research projects.

ACKNOWLEDGEMENTS

This manuscript is based on a project funded by the Federal Ministry for Economic Affairs and Climate Action as part of the "Edge Data Economy" technology program. We gratefully acknowledge our "DEER" project partners' support in this research. The authors would like to thank the German Federal Government, the German State Governments, and the Joint Science Conference (GWK) for their funding and support as part of the NFDI4Energy consortium. The work was partially funded by the German Research Foundation (DFG) – 501865131 within the German National Research Data Infrastructure (NFDI, www.nfdi.de).

REFERENCES

- Abdelhamid, A. M., Zakzouk, N. E., and El Safty, S. (2022). A Multi-Agent Approach for Self-Healing and RES-Penetration in Smart Distribution Networks. *Mathematics*, 10(13).
- Albarakati, A. J., Azeroual, M., Boujoudar, Y., EL Iysaouy, L., Aljarboub, A., Tassaddiq, A., and EL Markhi, H. (2023). Multi-Agent-Based Fault Location and Cyber-Attack Detection in Distribution System. *Energies*, 16(1).
- Arghandeh, R., Von Meier, A., Mehrmanesh, L., and Mili, L. (2016). On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews*, 58:1060–1069.
- Choi, I.-S., Hong, J., and Kim, T.-W. (2020). Multi-Agent Based Cyber Attack Detection and Mitigation for Distribution Automation System. *IEEE Access*, 8:183495–183504. Conference Name: IEEE Access.
- Eslami, A., Abdollahi, F., and Khorasani, K. (2022). Stochastic fault and cyber-attack detection and consensus control in multi-agent systems. *International Journal of Control*, 95(9):2379–2397. Publisher: Taylor & Francis. eprint: <https://doi.org/10.1080/00207179.2021.1912394>.

- Fang, Z. H., Mo, H. D., and Wang, Y. (2017). Reliability analysis of cyber-physical systems considering cyber-attacks. In *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pages 364–368, Singapore. IEEE.
- Frost, E., Heiken, J., Tröschel, M., and Nieße, A. (2024). Detecting and analyzing agent communication anomalies in distributed energy system control. pages 625–632.
- Frost, E., Radtke, M., Nebel-Wenner, M., Oest, F., and Stark, S. (2024). cosima-mango: Investigating Multi-Agent System Robustness Through Integrated Communication Simulation. *SoftwareX*.
- Frost, E., Veith, E. M., and Fischer, L. (2020). Robust and deterministic scheduling of power grid actors. In *2020 7th International Conference on Control, Decision and Information Technologies (CoDIT)*, volume 1, pages 100–105. IEEE.
- Hasanuzzaman Shawon, M., Muyeen, S. M., Ghosh, A., Islam, S. M., and Baptista, M. S. (2019). Multi-Agent Systems in ICT Enabled Smart Grid: A Status Update on Technology Framework and Applications. *IEEE Access*, 7:97959–97973. Conference Name: IEEE Access.
- Hines, P., Veneman, J., and Tivnan, B. (2014). Smart grid: Reliability, security, and resiliency. *University of Vermont*.
- Ilyes, N., Ben Smida, M., Khalgui, M., and Bachir, A. (2019). *Multi Agent System-based Approach for Enhancing Cyber-Physical Security in Smart Grids*.
- Kou, Y., Bie, Z., Li, G., Liu, F., and Jiang, J. (2021). Reliability evaluation of multi-agent integrated energy systems with fully distributed communication. *Energy*, 224:120123.
- Mahela, O. P., Khosravy, M., Gupta, N., Khan, B., Alhelou, H. H., Mahla, R., Patel, N., and Siano, P. (2022). Comprehensive overview of multi-agent systems for controlling smart grids. *CSEE Journal of Power and Energy Systems*, 8(1):115–131.
- Oest, F., Radtke, M., Blank-Babazadeh, M., Holly, S., and Lehnhoff, S. (2021). Evaluation of Communication Infrastructures for Distributed Optimization of Virtual Power Plant Schedules. *Energies 2021*, 14:1226.
- Radtke, M., Stucke, C., Trauernicht, M., Montag, C., Oest, F., Frost, E., Bremer, J., and Lehnhoff, S. (2023). *Integrating Agent-Based Control for Normal Operation in Interconnected Power and Communication Systems Simulation*. Pages: 233.
- Sanislav, T., Zeadally, S., Mois, G., and Fouchal, H. (2017). Multi-agent architecture for reliable Cyber-Physical Systems (CPS). In *2017 IEEE Symposium on Computers and Communications (ISCC)*, pages 170–175.
- Wang, P. and Govindarasu, M. (2020a). Multi-Agent Based Attack-Resilient System Integrity Protection for Smart Grid. *IEEE Transactions on Smart Grid*, 11(4):3447–3456.
- Wang, P. and Govindarasu, M. (2020b). Multi-agent based attack-resilient system integrity protection for smart grid. *IEEE Transactions on Smart Grid*, 11(4):3447–3456.
- Xiahou, K. S., Liu, Y., and Wu, Q. H. (2021). Robust Load Frequency Control of Power Systems Against Random Time-Delay Attacks. *IEEE Transactions on Smart Grid*, 12, 1:909–911.
- Xu, L., Guo, Q., Wang, Z., and Sun, H. (2021). Modeling of time-delayed distributed cyber-physical power systems for small-signal stability analysis. *IEEE Transactions on Smart Grid*, 12(4):3425–3437.
- Yang, Q., Chen, G., and Wang, T. (2020). ADMM-based distributed algorithm for economic dispatch in power systems with both packet drops and communication delays. *IEEE/CAA Journal of Automatica Sinica*, 7, 3:842–852.
- Yohanandhan, R. V., Elavarasan, R. M., Manoharan, P., and Mihet-Popa, L. (2020). Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications. *IEEE Access*, 8:151019–151064.
- Zhang, D., Feng, G., Shi, Y., and Srinivasan, D. (2021). Physical Safety and Cyber Security Analysis of Multi-Agent Systems: A Survey of Recent Advances. *IEEE/CAA Journal of Automatica Sinica*, 8(2):319–333.
- Zhou, T. L., Xiahou, K. S., Zhang, L. L., and Wu, Q. H. (2021). Multi-agent-based hierarchical detection and mitigation of cyber attacks in power systems. *International Journal of Electrical Power & Energy Systems*, 125:106516.
- Zhu, Y., Li, H., Duan, H., and Guan, X. (2019). Optimal Energy Consumption for Consensus of Multi-Agent Systems With Communication Faults. *IEEE Access*, 7:138941–138949. Conference Name: IEEE Access.