The Role of Architectures and Information Availability for Anomaly Detection in Cyber-Physical Energy Systems

Emilie Frost[1,2][a] and Astrid Nieße[1][b]
[1]*Department of Computing Science, Carl von Ossietzky Universität Oldenburg, Ammerländer Heerstraße 114-118, Oldenburg, Germany*
[2]*Distributed Artificial Intelligence, OFFIS - Institute for Information Technology, Escherweg 2, Oldenburg, Germany*
{*emilie.frost, astrid.niesse*}*@uni-oldenburg.de*

Keywords: Anomaly Detection, Controlled Self-Organization, Cyber-Physical Energy Systems.

Abstract: In the context of Cyber Physical Energy Systems (CPES), anomaly detection is an important requirement for dealing with the increasing threats of cyber-attacks. However, privacy or regulatory restrictions might limit the access of information for performing anomaly detection. This paper discusses different possible architectures for the development of an anomaly detection observer in CPES, in the context of information availability. Using an agent-based control use case, these architectures, information availability and their impact on anomaly detection performance are evaluated. The results shed light on the design of appropriate architectures for anomaly detection in CPES with the aim of improving the overall robustness of the system.

1 INTRODUCTION

Current energy systems are evolving into Cyber Physical Energy Systems (CPES), where physical components of the power grid are integrated with Information and Communication Technology (ICT) systems. These ICT systems are designed to monitor, control and optimize the performance (Hasanuzzaman Shawon et al., 2019). With the increasing decentralization resulting from energy transition, these control systems must also address decentralized structures. In this context, Multi-Agent Systems (MAS) are often applied in CPES (Taleb et al., 2023; Denysiuk et al., 2020), as these are well suited to implement distributed system concepts (Ren et al., 2021) and allow for self-organization, or even self-healing, in safety-critical applications (Nieße and Tröschel, 2016; Dehghanpour et al., 2017). However, the strong interdependencies between power and ICT system not only bring advantages but also lead to new threats coming from the ICT side, as for example cyber attacks (Yohanandhan et al., 2020; Zhu, 2019). The necessity to recognize errors and deviations from plan or operation is therefore becoming more urgent. This emphasizes the need for anomaly detection, as a prerequisite to react to threats and disturbances (Anwar and Mahmood, 2014). In order to ensure robustness against disturbances and attacks in self-organizing systems, concepts of Organic Computing (OC) can be applied (Chaaban et al., 2013; Kantert et al., 2017). Here, an observer/controller architecture is used to observe and control the system in order to achieve controlled self-organization, i.e., the self-organization of the system is given, while it is possible to react in case of deviations from the desired behavior (Richter et al., 2006). An observer is proposed, which measures and quantifies emergent behavior of the system (Richter et al., 2006). Thus, the observer can also perform anomaly detection. However, the observer performs its task based on the available information of the system (Richter et al., 2006). Especially in CPES, some information might not be available to the observer, as regulatory restrictions or reasons such as privacy and data protection might limit the access to information. Depending on the use case, different observer architectures are suitable. However, typically, just one architecture is implemented in literature: a centralized or distributed anomaly detection. In particular, multi-leveled or hierarchical architectures are only discussed in theory. Tomforde et al. (2011) discuss different architectures of observers (and controllers) for OC systems, stating that the designer should choose the architecture based on the system's size, complexity and heterogeneity. However, when applying OC to CPES, the available information also

[a] https://orcid.org/0000-0003-4791-2333
[b] https://orcid.org/0000-0003-1881-9172

Frost, E. and Nieße, A.
The Role of Architectures and Information Availability for Anomaly Detection in Cyber-Physical Energy Systems.
DOI: 10.5220/0013371400003890

In *Proceedings of the 17th International Conference on Agents and Artificial Intelligence (ICAART 2025) - Volume 1*, pages 671-678
ISBN: 978-989-758-737-5; ISSN: 2184-433X

needs to be considered when choosing the best suitable architecture.

For that reason, this paper discusses architectures for anomaly detection in CPES, assuming different levels of information availability. To do so, an implementation of an agent-based control use case is presented, considering communication effects on the system. The implementation was used to perform experiments with different architectures and thus different levels of information availability. This allowed the effects on detection performance to be studied and the suitability of different architectures to be evaluated. The contributions of this paper are the following:

- We provide datasets for anomaly detection for an agent-based control use case in CPES, considering a cyber attack on the agent system, based on the analysis presented by Frost and Nieße (2024). These datasets can serve as a basis for further investigations into the detection of anomalies and the influence of cyber attacks on MAS.
- Possible architectures for an observer for CPES are derived from the literature and discussed.
- Different layers of information that are available for anomaly detection are addressed.
- In addition, we investigate the impact of the defined architectures and the availability of information on the performance of anomaly detection. The results are also used to evaluate architectures and the suitability of combining these, e.g., as multi-leveled architectures. The proposed architectures, information layers, and results provide a basis for a stable and appropriate design of anomaly detection in CPES.
- A recommendation for the design of an architecture for CPES is made, which can be built upon in future work for robust detection of anomalies in CPES, based on given constraints of the respective use case.

The paper is organized as follows. In section 2, we present related work regarding anomaly detection architectures. Afterward, in section 3, architectures for CPES are discussed, including the declaration of levels of information available. The details of the implementation are described in section 4, followed by the evaluation in section 5. The paper ends with the discussion in section 6 and the conclusion in section 7.

2 RELATED WORK

In this section, related work regarding architectures for anomaly detection is discussed. Architectures for an observer performing anomaly detection can be derived from from OC systems. Richter et al. (2006) present a general architecture, which can be used in a centralized, distributed or multi-leveled way. The different architectures are discussed regarding the affected control parameters and controlled elements. Tomforde et al. (2011) extend the discussion by presenting the architectures for the observer (and controller): the centralized architecture considers a single observer taking into account various components, a distributed observer is implemented for each component and the multi-leveled architecture contains a highest instance to define goals, while lower layers convert these into more specific goals. Haehner et al. (2013) explicitly discuss architectural concepts for anomaly detection, using OC. The authors discuss local and cooperative anomaly detection.

For anomaly detection in sensor systems, Erhan et al. (2021) present the following architectures: centralized, distributed, collaborative decentralized, or between fully decentralized and fully centralized, processing information immediately.

Tan et al. (2020) discuss typical control structures for attack detection. The authors distinguish between a centralized architecture that requires global information knowledge from all control units, a decentralized architecture (no information from other parts of the system is given), a distributed architecture, which contains knowledge from local measurements and neighbor units (measurements are communicated) and a hierarchical architecture, in which an additional secondary detection is centralized as global information from all essential units is required.

To sum up, previous works consider the architectures for anomaly detection listed in the following. Some authors also discuss the option for collaborative anomaly detection, which can refer to different architectures (Erhan et al., 2021).

- **Centralized Anomaly Detection.** Global information knowledge from all control units is considered (Tan et al., 2020).
- **Decentralized Anomaly Detection.** This architecture is implemented separately for each component (Tomforde et al., 2011), no information from other parts of the system is given (Tan et al., 2020).
- **Distributed Anomaly Detection.** This architecture considers knowledge from local measurements and from neighbors (knowledge is communicated) (Tan et al., 2020).
- **Multi-Leveled / Hierarchical Anomaly Detection.** Here, an additional secondary instance is centralized, considering global information (Tan

et al., 2020), which defines goals as the highest instance, while the lower layers convert these into more specific goals (Tomforde et al., 2011).

However, the aforementioned approaches only discuss different variations, none of the approaches implement architectures and investigate their effects. Anomaly detection methods in CPES are mostly implemented either in a centralized (Turowski et al., 2022; Fu et al., 2022) or decentralized architecture (Gupta et al., 2021; Ramanan et al., 2022), without discussing other options or comparing architectures. In particular, the option of multi-leveled architectures has only been discussed in the presented literature, but never implemented or evaluated.

In previous work, Frost et al. (2024) compare the effects of two anomaly detection architectures: centralized and distributed. The authors discuss the effect of having insight into the exchanged messages of an agent-based system. The results show that the chosen architecture and the available information have a significant impact on the performance of anomaly detection. However, the authors only investigate the effect of available information partially, only regarding insights into the messages. Additionally, only an example of an attack implementation is shown. Overall, the authors only investigate two architectures. The option to take into account multi-leveled architectures, considering available information, is not discussed and is therefore evaluated in this paper. To do so, the performance of multiple architectures is discussed regarding different information available, and combinations for multi-leveled architectures are derived. The information and architectures available for this purpose are described in the following section.

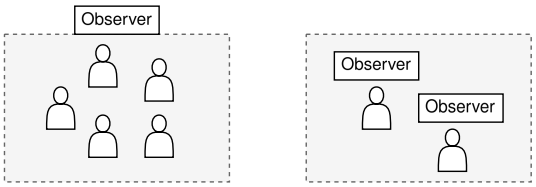
3 OBSERVER ARCHITECTURES IN CYBER-PHYSICAL ENERGY SYSTEMS

In this section, possible architectures for anomaly detection in CPES are discussed. Additionally, different levels of information availability are presented.

When applying the presented possible architectures for anomaly detection in the literature to CPES, access to information might be limited. In such decentralized systems, due to privacy or data protection, some information, especially regarding local device-specific data of a Distributed Energy Resource (DER), might not be available. The architectures and their assumptions regarding the information taken into account can therefore not be applied to the CPES for all use cases. The assumption on the centralized architecture, that global information knowledge from all units is given, as presented by Tan et al. (2020), is not always suitable for CPES. This information might not include specific local information, such as device-specific data or unit constraints. Instead, it might be possible that selected information is available at a central location, while other information might only be available locally, especially when considering agent-based systems for distributed control in CPES. Often, each agent represents a DER or its flexibility (Ding et al., 2024), for optimization, agents communicate with each other and exchange information. However, the available information is not communicated completely, only selected information, in order to preserve privacy or communication overhead (Bremer and Lehnhoff, 2019). This way of optimization allows keeping technical details and constraints locally (Stark et al., 2024). Because the information on which the detection is based may be reduced, this affects how anomalies are detected.

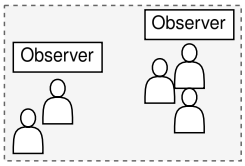
Thus, in order to perform anomaly detection in CPES, it is essential to discuss the suitability of certain architectures depending on the information available. Regarding the performance of different architectures, several combinations for hierarchical or multi-leveled architectures can be considered. For these architectures, multiple variations are possible, depending on the number of nodes and information available. In the literature, multi-leveled approaches add centralized detection to existing decentralized detection methods (Tan et al., 2020). When considering anomaly detection in a distributed system, more variations can be possible, especially when considering agent-based control in CPES use cases. For example, multiple single wind plants in the system might be controlled by one operator. Therefore, some information might be available grouped in one place, e.g., per unit type. For this reason, we decided to additionally investigate the architecture of an observer grouped per unit type. To investigate the influence of different architectures, we additionally assume a further grouped architecture, which considers a number of randomly chosen units. This results in a total of four different architectures to be investigated, depicted in Figure 1.

- Centralized anomaly detection (Figure 1a): this architecture considers data of the whole network.
- Decentralized anomaly detection (Figure 1b): data of individual units is considered.
- Grouped by unit type (Figure 1c): this architecture considers data of a certain unit type (e.g., wind, photovoltaic (PV)).
- Grouped randomly (also Figure 1c): data of a random group of units is considered.



(a) Centralized anomaly detection

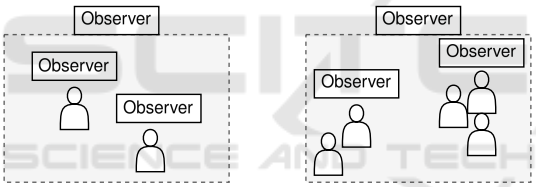
(b) Decentralized anomaly detection



(c) Grouped anomaly detection

Figure 1: Architectures for anomaly detection in agent systems.

Possible multi-leveled or hierarchical architectures can now be built by adding a centralized observer to the decentralized (Figure 2a) or grouped architecture (Figure 2a).



(a) Multi-leveled decentralized

(b) Multi-leveled grouped

Figure 2: Multi-leveled architectures for anomaly detection in agent systems.

All architectures can be expanded to include communication between observers. To evaluate different architectures, their performance must be investigated given the different information available. To do so, four levels of information availability are assumed, depicted in Figure 3 and described in the following.

When considering agent-based control in CPES, agents communicate with each other to perform the optimization of a certain task. To do so, messages are exchanged. However, access to the content of these messages can not always be assumed. The first level of information therefore only considers the agent sending the message and the timestamp, similar to the investigations in Frost et al. (2024). The second level additionally considers communication information, such as delays of exchanged messages and traffic information. Still, no insight into the message is given, but information about the arrival and sending

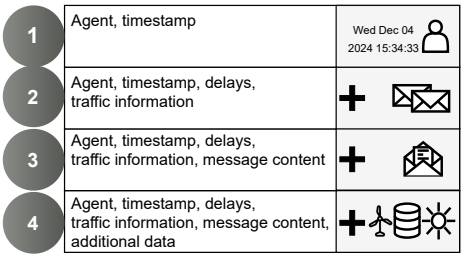


Figure 3: Levels of information assumed to be available for the anomaly detection.

of all messages is essential. The third level assumes that insight into the message is given; the content of the message is considered. The last level extends the third level with additional information. This can contain constraints or the current state of the unit, or forecast data regarding weather, power, or load.

In CPES, anomaly detection may require different information for different types of attacks. The first two levels are relevant to detect any kind of attack on the communication behavior, such as Denial-of-Service (DoS) attacks that cause delays or missing messages, while this does not apply to attacks that target the message content.

4 ANOMALIES IN AGENT-BASED SYSTEMS

In the following, the implementation of the anomaly detection architectures is presented. To investigate anomalies in agent-based systems in CPES, we chose the practical implementation presented in Frost and Nieße (2024), which is publicly available[1]. The use case is self-consumption optimization of a neighborhood grid (energy community), represented by a MAS, considering redispatch requests from a grid operator. The use case is therefore based on the system concepts presented by Krueger et al. (2023); Radtke et al. (2023). Each agent controls a selected DER or household. Additionally, the implementation contains a communication simulation, which enables a realistic investigation of the ICT systems effects. The realistic environment allows real-world conditions such as delayed messages and message failures to be considered. Anomaly detection can therefore learn such conditions and be better applied to practical cases.

Selected effects of cyber attacks affecting the agent system are also considered in the implementation in Frost and Nieße (2024). For the detection of anomalies, we refer to the implementation of com-

[1]https://github.com/Digitalized-Energy-Systems/communication-incidents-in-cpes

promised process data, as this incident has particular relevance for the information layers. It is implemented as the effect of selected cyber attacks, e.g., false data injection attacks, which are considered the most dangerous cyber attacks in smart grids (Amin et al., 2021), thus representing a particularly threatening incident. Power values in exchanged messages in the agent system are manipulated to consider compromised data, for one generation agent representing a wind plant, as described in Frost and Nieße (2024).

The datasets consider a day in July 2023 and are publicly available[2]. An overview of the datasets is given in Table 1.

Table 1: Overview of datasets for anomaly detection.

Data	Time	Messages	Anomalies
Normal	July 2023	540.000	0%
Compromised	July 2023	60.000	1%

To perform anomaly detection, a transformer autoencoder was implemented (Vaswani, 2017). Previous work found that the autoencoder, among others, predominantly achieved best results (Frost et al., 2024) and the transformer autoencoder is considered as a promising approach due to good performances in anomaly detection (Xu, 2021). The implementation of the detector was published, containing details of the configuration[3]. For the evaluation of different anomaly detection architectures, we refer to those presented in section 3. The architectures including the considered data are listed in the following.

- Centralized anomaly detection: data of the whole network is considered.
- Decentralized anomaly detection: data of only one component is assumed (here: the manipulated wind agent is considered).
- Grouped per unit type: data of one unit type is given (here: wind units are considered).
- Grouped randomly: data of a group of units is considered. The group was built randomly and considers wind, PV, battery, and household units.

In the evaluation, the architectures are investigated regarding the performance given the information available, as presented in Figure 3. For the fourth layer, in which additional information, as unit constraints or forecast data is added, we consider the constraints of the unit, i.e., the technical limitations of the power.

[2]https://zenodo.org/records/14333637

[3]https://gitlab.com/digitalized-energy-systems/models/detection-and-prediction-of-communication-incidents-in-cpes

5 EVALUATION

In this section, the performances of the different anomaly detection architectures are presented. Although the anomalies are in the performance values within the messages, not only the information levels that require access to the messages are analyzed. If an agent sends manipulated values, other agents react differently, affecting the behavior of others and the duration of the overall optimization. The compromised data therefore also influences other parameters than those only recognizable in the message content (such as the solution quality). As shown in Frost and Nieße (2024), there are effects on the optimization and transmission duration of the messages. For this reason, the first two levels of information, assuming insight into the messages, are also evaluated to assess whether the changes in behavior can be detected. For the results, precision, recall, and F1-score are discussed. For completeness, the specificity of the anomaly detection performance was also examined. True negative entries appear easily recognizable (specificity always above 0.8). However, this can be explained by the imbalanced dataset, so we focus on the other metrics for discussion.

Centralized Anomaly Detection. The performance of the centralized anomaly detection can be seen in Table 2 for all information levels. It is visible, that the centralized architecture does not succeed in recognizing the anomalies satisfactorily. With no insight into the messages (levels 1 and 2), the results are very poor (no metric above 0.7, most below 0.2). Adding the message content to the detection data improves the performance, while additionally adding the constraints does not make much difference (metrics between 0.58 and 0.77). Overall, the centralized architecture does not reliably detect anomalies.

Table 2: Centralized architecture.

Information Level	Precision	Recall	F1-Score
1 (Agent, time)	0.17	0.52	0.26
2 (Delays)	0.10	0.67	0.17
3 (Content)	**0.77**	**0.58**	**0.66**
4 (Constraints)	**0.76**	**0.60**	**0.68**

Decentralized Anomaly Detection The results of the decentralized anomaly detection are shown in Table 3. Here, too, it can be seen that the anomalies cannot be detected without having the content of the messages available (only recall above 0.7). Insight into the messages improves the performance (all metrics higher than 0.8). Adding the unit constraints to

the data again leads to improvements. The decentralized anomaly detection achieves the overall best results and satisfactory results (all metrics above 0.8). The high precision is striking; the detected anomalies appear to be correct. The value for recall is worse; some anomalies do not appear to have been detected.

Table 3: Decentralized architecture.

Information Level	Precision	Recall	F1-Score
1 (Agent, time)	0.10	0.73	0.12
2 (Delays)	0.15	0.36	0.21
3 (Content)	**0.91**	**0.80**	**0.85**
4 (Constraints)	**0.91**	**0.89**	**0.90**

Anomaly Detection per Unit Type Group. Table 4 shows the results of the anomaly detection performed on data for one unit type group (wind devices). The results are, again, very poor without insights into the messages (only recall above 0.7). However, also given the content and additional information, the results are worse than those achieved by the decentralized architecture. It can be concluded that the joint consideration of units which have similar behavior, since the respective DER have similar conditions, does not result in any advantages in this case.

Table 4: Grouped unit type.

Information Level	Precision	Recall	F1-Score
1 (Agent, time)	0.13	0.76	0.22
2 (Delays)	0.13	0.76	0.22
3 (Content)	**0.92**	**0.47**	**0.62**
4 (Constraints)	**0.92**	**0.52**	**0.66**

Anomaly Detection for a Random Group of Units. The results of the anomaly detection performed for a random group of DER is shown in Table 5. The results are very similar to those of the grouping by unit type: insight into messages leads to better results, however, the architecture performs worse than the decentralized architecture (F1-score still below 0.7). These results support the thesis that grouping the systems does not bring any advantages with regard to the detection of anomalies.

Table 5: Grouped randomly.

Information Level	Precision	Recall	F1-Score
1 (Agent, time)	0.23	0.72	0.35
2 (Delays)	0.32	0.70	0.44
3 (Content)	**0.86**	**0.47**	**0.61**
4 (Constraints)	**1.0**	**0.49**	**0.66**

6 DISCUSSION

When comparing the performance, overall, it is noticeable that all architectures achieve very poor results if no insight into the messages is given. Thus, it can be assumed that changes in the values (compromised process data) are not recognizable in the communication behavior of the agents. These information levels (1 and 2) can still provide added value for attacks affecting the communication behavior of the agents, such as DoS attacks. The fact also emphasizes the relevance of a decentralized architecture in CPES, as local information cannot be assumed to be guaranteed for anomaly detection. Overall, the best results are found by the decentralized anomaly detection. This type of architecture seems to be the most suitable for anomalies related to compromised process data. This can presumably be explained by the fact that the decentralized architecture is tailored to the behavior of a single agent and can therefore presumably learn its behavior better since only the relevant information required to detect its compromised data is considered.

The results also show that grouping the agents (either randomly or by unit type) for anomaly detection does not provide any added value. Communication between the observers for anomaly detection randomly or in DER area (neighboring agents) is therefore not considered particularly promising. In addition, this exchange would entail a communication overhead that could have a detrimental effect on the system (delays, later response times due to increased time to detection). Combining two detection approaches into a multi-leveled one therefore only makes sense for centralized and decentralized detection approaches.

In previous work, anomalies regarding the communication behavior of agents were investigated (Frost et al., 2024). There, distributed and centralized architectures were compared. It was found that none of the architectures was more suitable; some characteristics of the anomalies were better detected by the centralized architecture, others vice versa.

Considering the results of the previous work and this paper, the relevance of multi-leveled or hierarchical architectures becomes apparent. Different cyber attacks have different effects on the agent system; in addition to changes in values and communication behavior, agents or communication links fail. To detect multiple types of attacks, architectures can be combined. Multi-leveled architectures typically contain a centralized observer in addition to, for example, the decentralized instance. The centralized observer monitors the entire system, e.g., without having insight into the messages, in addition, decentral-

ized anomaly detection is implemented for each node, where insight into the messages is assumed (at least level 3). The proposed architecture including the available information for each observer is shown in Figure 4. The decentralized observer considers all locally available information, which may include additional information such as forecast data or constraints.

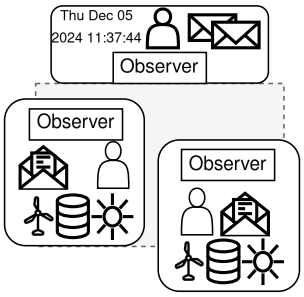


Figure 4: Proposed multi-leveled architecture.

The anomalies detected by both observers can serve as the basis for the reaction. For example, ensemble learning, which combines the results of different models, could be considered for selecting the anomalies. Finally, the results of both observers provide a good basis for a controller to make decisions. The results can be communicated to a controller (either local or central), which can decide based on the detected anomalies and the information available. Again, different (controller) architectures need to be explored. This enables collaborative anomaly detection while respecting privacy constraints, as local information does not need to be shared. Furthermore, no communication overhead is caused, as current values do not need to be exchanged between observers in addition to the exchanged messages.

7 CONCLUSION

This paper presents and evaluates different architectures for designing an observer to perform anomaly detection in CPES. The impact of different available information on the detection performance is investigated. The results show that compromised data is only detected when insight into the messages is provided. This shows the importance of decentralized anomaly detection, since some information, such as local DER constraints, may not be available at a central location in CPES. The need for decentralized anomaly detection is additionally emphasized by the fact that this type of architecture outperforms the others. The results show that access to information must be considered when choosing an architecture for an observer. Additionally, the need for multi-leveled architectures for anomaly detection in CPES is emphasized, as different information is available at different locations. Our results and findings support a robust observer design, according to customized and adaptable circumstances, thus, addressing the challenges of anomaly detection in CPES by providing a basis for reliable anomaly detection. Our findings can be used to implement a controller, which takes reaction to anomalies, based on the results of a multi-leveled architecture. The discussed architectures must also be compared in terms of controller implementation. Future work can build on our work to investigate the impact of architectures and information access on anomaly prediction, as part of the observer in OC systems is the prediction of the systems' behavior. Accurate predictions simplify reacting to detected anomalies, thereby improving the overall robustness of the system.

ACKNOWLEDGEMENTS

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

Amin, M., El-Sousy, F. F., Aziz, G. A. A., Gaber, K., and Mohammed, O. A. (2021). Cps attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review. *Ieee Access*, 9:38571–38601.

Anwar, A. and Mahmood, A. N. (2014). Cyber security of smart grid infrastructure. *CoRR*, abs/1401.3936.

Bremer, J. and Lehnhoff, S. (2019). Lazy agents for large scale global optimization. In *ICAART (1)*, pages 72–79.

Chaaban, Y., Müller-Schloer, C., and Hähner, J. (2013). Robustmas: Measuring robustness in hybrid central/self-organising multi-agent systems. *International Conference on Advanced Cognitive Technologies & Applications*.

Dehghanpour, K., Colson, C., and Nehrir, H. (2017). A survey on smart agent-based microgrids for resilient/self-healing grids. *Energies*, 10(5):620.

Denysiuk, R., Lilliu, F., Vinyals, M., Reforgiato, D., et al. (2020). Multiagent system for community energy management. In *Proceedings of the 12th International Conference on Agents and Artificial Intelligence-*

Volume 1, volume 1, pages 28–39. Scitepress, Science and Technology Publications.

Ding, B., Li, Z., Li, Z., Xue, Y., Chang, X., Su, J., Jin, X., and Sun, H. (2024). A ccp-based distributed cooperative operation strategy for multi-agent energy systems integrated with wind, solar, and buildings. *Applied Energy*, 365:123275.

Erhan, L., Ndubuaku, M., Di Mauro, M., Song, W., Chen, M., Fortino, G., Bagdasar, O., and Liotta, A. (2021). Smart anomaly detection in sensor systems: A multi-perspective review. *Information Fusion*, 67:64–79.

Frost, E., Heiken, J. C., Tröschel, M., and Nieße, A. (2024). Detecting and analyzing agent communication anomalies in distributed energy system control. In *ICAART (3)*, pages 625–632.

Frost, E. and Nieße, A. (2024). Communication incidents in self-organising cyber-physical energy systems: Assessing robustness. In *5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES)*, pages 1–6.

Fu, C., Arjunan, P., and Miller, C. (2022). Trimming outliers using trees: winning solution of the large-scale energy anomaly detection (lead) competition. In *Proceedings of the 9th ACM International Conference on Systems for Energy-Efficient Buildings, Cities, and Transportation*, pages 456–461.

Gupta, K., Sahoo, S., Mohanty, R., Panigrahi, B. K., and Blaabjerg, F. (2021). Decentralized anomaly characterization certificates in cyber-physical power electronics based power systems. In *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*, pages 1–6.

Haehner, J., Rudolph, S., Tomforde, S., Fisch, D., Sick, B., Kopal, N., and Wacker, A. (2013). A concept for securing cyber-physical systems with organic computing techniques. In *26th International Conference on Architecture of Computing Systems 2013*, pages 1–13.

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.

Kantert, J., Tomforde, S., Müller-Schloer, C., Edenhofer, S., and Sick, B. (2017). Quantitative robustness-a generalised approach to compare the impact of disturbances in self-organising systems. In *ICAART (1)*, pages 39–50.

Krueger, C., Otte, M., Holly, S., Rathjen, S., Wellssow, A., and Lehnhoff, S. (2023). Redispatch 3.0–congestion management for german power grids–considering controllable resources in low-voltage grids. In *ETG Congress 2023*, pages 1–7. VDE.

Nieße, A. and Tröschel, M. (2016). Controlled self-organization in smart grids. In *2016 IEEE International Symposium on Systems Engineering (ISSE)*, pages 1–6. IEEE.

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. In *2023 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 228–233. IEEE.

Ramanan, P., Li, D., and Gebraeel, N. (2022). Blockchain-based decentralized replay attack detection for large-scale power systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 52(8):4727–4739.

Ren, Y., Yu, J., Zhao, A., Jing, W., Ran, T., and Yang, X. (2021). A multi-objective operation strategy optimization for ice storage systems based on decentralized control structure. *Building Services Engineering Research and Technology*, 42(1):62–81.

Richter, U., Mnif, M., Branke, J., Müller-Schloer, C., and Schmeck, H. (2006). Towards a generic observer/controller architecture for organic computing. *INFORMATIK 2006–Informatik für Menschen, Band 1*, pages 112–119.

Stark, S., Frost, E., and Nebel-Wenner, M. (2024). Distributed multi-objective optimization in cyber-physical energy systems. *ACM SIGENERGY Energy Informatics Review*, 4(2):7–18.

Taleb, I., Guerard, G., Fauberteau, F., and Nguyen, N. (2023). A holonic multi-agent architecture for smart grids. In *ICAART (1)*, pages 126–134.

Tan, S., Guerrero, J. M., Xie, P., Han, R., and Vasquez, J. C. (2020). Brief survey on attack detection methods for cyber-physical systems. *IEEE Systems Journal*, 14(4):5329–5339.

Tomforde, S., Prothmann, H., Branke, J., Hähner, J., Mnif, M., Müller-Schloer, C., Richter, U., and Schmeck, H. (2011). Observation and control of organic systems. *Organic computing—a paradigm shift for complex systems*, pages 325–338.

Turowski, M., Heidrich, B., Phipps, K., Schmieder, K., Neumann, O., Mikut, R., and Hagenmeyer, V. (2022). Enhancing anomaly detection methods for energy time series using latent space data representations. In *Proceedings of the Thirteenth ACM International Conference on Future Energy Systems*, pages 208–227.

Vaswani, A. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*.

Xu, J. (2021). Anomaly transformer: Time series anomaly detection with association discrepancy. *arXiv preprint arXiv:2110.02642*.

Yohanandhan, R., Elavarasan, R., 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, vol. 8*, pages 151019–151064.

Zhu, Q. (2019). Multilayer cyber-physical security and resilience for smart grid. *Smart grid control: overview and research opportunities*, pages 25–239.