More secure processes with decentralised AI

Using the example of automated monitoring of energy substations

Mirko Düssel, Samuel T. Stähle, ChatGPT 4.0, Oktober 2nd 2024

Table of Contents

Introduction

In September 2024, Samuel Stähle, CEO PowerBrain.Shop®, Mirko Düssel, Mirko Düssel & Co. Interdisciplinary Management Consultants, and ChatGPT4o discussed the question of how automated monitoring based on AI solutions leads to more efficient and safer processes. The authors have many years of practical experience in the implementation of AI applications in the areas of maintenance, process engineering and strategy and help companies and organisations to recognise and exploit the concrete potential of artificial intelligence (AI). The insights gained are reflected on the example of the automation of power distribution and transmission substations and discussed with ChatGPT.

The demands placed on infrastructure operators such as energy supply companies are constantly increasing. Electrical energy should be available everywhere and at all times and be produced from renewable energy sources, with unlimited capacity and at low cost. The need for energy grid automation is therefore constantly increasing. Key drivers for real improvements in efficiency include technologies based on the effective use of Artificial Intelligence (AI).

Energy supply systems are of crucial importance for countries and regions and must always work reliably. When automating these systems, the question arises as to how the software architecture used should best be structured in order to ensure maximum reliability and minimum downtime of power supply.

It also needs to be clarified whether it is more advantageous to operate the artificial intelligence centrally at one location or distributed at several decentralised locations. We discussed these considerations together with ChatGPT4o.

As sophisticated software is often initially used in large data centres, it is now common practice in 2024 to operate artificial intelligence centrally in such facilities.

Advantages of centralised AI

Centralised artificial intelligence has a number of advantages that can be very attractive in certain scenarios.

1. **Concentration of resources**

   Considerable computing resources can be concentrated in a centralised system in order to train complex models and process large amounts of data. This enables the use of powerful supercomputers and specialised hardware such as GPUs and TPUs.

2. **Simpler management and maintenance**

   A centralised system simplifies management and maintenance as all updates, patches and improvements are carried out in one central location only. This leads to more consistent and better controlled systems.

3. **Efficiency and consistency**

   Centralised systems provide a uniform platform for data processing and model development, which leads to consistent results and efficient processes. Data and models do not have to be duplicated or synchronised multiple times.

4. **Access to extensive data sets**

   Centralised AI systems often have access to large, comprehensive data sets, which can lead to more accurate and powerful models. Centralised data storage enables more comprehensive data analysis and use.

5. **Coordination and collaboration**
   A centralised system facilitates coordination and collaboration between different teams and departments. Everyone involved can access the same resources and information, which increases the efficiency and effectiveness of the work.

6. **Cost efficiency for certain applications**
   For certain applications and organisations, a centralised system can be more cost-efficient, especially when it comes to using specialised hardware and software that cannot be easily transferred to distributed systems.
7. **Scalability through cloud services**
   Centralised AI can be easily scaled by using cloud services. Cloud providers offer flexible and scalable infrastructures that make it possible to expand or reduce computing resources as required.
8. **Faster development and deployment**
   As all resources are centralised, new models and applications can be developed and deployed faster. This is particularly beneficial in fast-moving industries where time is a critical factor.
9. **Quality assurance of AI training data sets**
   As all training data is stored centrally, its suitability for achieving a target model or its quality can be influenced.

These advantages make centralised AI an attractive solution for many organisations, especially in scenarios where large amounts of data need to be processed and central control is an advantage.

This raises the question of what the disadvantages of using centralised AI might be.

Disadvantages of centralised AI

Centralised AI systems undoubtedly offer many advantages. But what disadvantages must be taken into account?

1. **High latency times**
   - **Delays in data transmission:** As data has to be transferred from end devices to central servers and back again, delays can occur, which is particularly problematic for time-critical applications.
   - **Dependence on network connections:** The performance of centralised AI systems depends heavily on the quality and stability of network connections. Unstable or slow connections can significantly affect response times.
   - **Cloud applications and dependence on Internet availability:** If the network connections are established via the Internet (fixed and mobile), the aforementioned problems are exacerbated.
2. **High infrastructure and operating costs**
   - **Costs for data centres:** The operation and maintenance of large central data centres is expensive. This includes costs for hardware, electricity, cooling and personnel.

- **Bandwidth costs:** The transfer of large amounts of data between end devices and centralised servers can result in high bandwidth costs.

3. **Scaling problems**
   - Limited scalability: Centralised systems often struggle to scale with a rapidly growing number of end devices and users, which can lead to performance degradation.
   - Bottlenecks: Centralised architecture can lead to bottlenecks when demand exceeds the capacity of the central servers.
4. **Data security and data protection issues**
   - **Centralised attack targets:** Centralised data centres are attractive targets for cyber attacks. A successful attack can compromise large amounts of sensitive data and exclude many users from using it at the same time.
   - **Data protection risks:** Transferring sensitive data to centralised servers can increase data protection risks, especially if the data is sent across international borders.
5. **Limited adaptability**
   - **Slow adaptation to local conditions:** Centralised AI systems have difficulty adapting quickly to specific local requirements and conditions because the models are trained and managed centrally.
   - **Lack of flexibility:** Changes and adaptations often require extensive changes to the central infrastructure, which can be time-consuming and expensive.
6. **Dependence on centralised services**
   - **Single point of failure:** Central systems represent a single point of failure. A problem or failure in the central data centre can affect the availability of the services as a whole.
   - **Service availability:** The availability of centralised services can be massively jeopardised by external factors such as natural disasters or network disruptions.
7. **Regulatory and legal challenges**
   - **Data storage and transfer:** Storing and transferring data across international borders can pose regulatory and legal challenges, particularly with regard to data protection laws such as the GDPR (General Data Protection Regulation) or DSA (Digital Services Act).

These disadvantages of centralised AI systems make them appear less suitable in many cases. This applies in particular to energy automation use cases that require very fast response times, high flexibility, strong data protection and very high cyber security.

In such scenarios, a decentralised architecture may be the better alternative.

Example: Power Transmission and Distribution Substations

From the perspective of operators of investment-intensive substations, which CAPEX are usually in the single-digit million Euro range, real-time monitoring is of great importance. The aforementioned latencies and bandwidth limitations in real-time streaming of, for example, 10 infrared video cameras and 10 optical video cameras in parallel to just one central AI via mobile communications are particularly problematic here. Especially in regions without a correspondingly very broadband communication infrastructure such as optical fibre, for example.

If, for example, a transformer develops abnormal temperature hotspots due to short-term overload, wear and tear, insufficient maintenance, short circuits due to defective external insulators, connections or defective internal windings, lightning strikes, insufficient earthing, corrosion, or loose points, particularly at connections of the high-voltage conductors or cables, or even vandalism, etc., this must be detected very quickly. It is the only way to initiate any immediate measures, warnings or alarms before systems or components are damaged and the power transformer investment burns down in a large fireball and a regional power blackout occurs with significant impact on the quality of life for the regional population and infrastructure such as hospitals and police stations, for example.

AI monitoring to prevent the explosion of voltage transformers (potential transformers (PT)) or current transformers (CT) is just as time-critical. Faulty insulation and the ingress of moisture and dust, oil leakage, an overloaded dielectric or loose or corroded connections to high-voltage cables can lead to the rapid and spontaneous development of hot spots, which require prompt detection and immediate intervention to prevent significant damage of substation assets.

AI monitoring helps prevent, for example, ceramic parts of the outer insulator from being blown to pieces and the debris from being scattered over an area of up to 200 metres, damaging other components of the transformer substation and escalating the problem further until, in the worst case, there is a risk to life and limb.

These examples illustrate that prompt AI recognition and AI enabled reaction are essential in the energy industry and cannot depend on Internet service availability or quality.

How can Artificial Intelligence be decentralised?

The decentralisation of artificial intelligence can be achieved in various ways to improve the control, distribution and security of the solutions. Here are some of the main approaches:

1. **Edge Computing**: AI models are executed directly on local devices or close to the source of the data instead of in central data centres. This reduces latency times, improves data security (as data does not have to be sent to central servers) and enables significantly faster processing.
2. **Federated Learning**: AI models are trained on many decentralised devices or servers, whereby only the model updates and not the raw data are exchanged. This protects the privacy of users, as their data remains on their own local devices.
3. **Peer-to-Peer (P2P) Networks**: In a P2P network, the AI is distributed across many equivalent nodes that work together. Each node contributes to processing and learning without the need for a centralised server. This increases redundancy and security as the system is less susceptible to individual failures.
4. **Decentralized Cloud-Infrastructures**: Instead of central data centres, AI models can be run on a distributed cloud infrastructure that is spread across different geographical locations. This helps increase the robustness and security of the system as there is not one centralised dependency.
5. **Hybrid models**: A combination of centralised and decentralised approaches, where some parts of the AI infrastructure remain centralised while others are decentralised. This can provide a balance between efficiency, control and security.

Each of these approaches to decentralisation has its own advantages and challenges and can be used depending on the respective use case and its specific requirements.

Decentralising AI with edge computing

The most consistent and efficient decentralisation of AI is achieved with edge computing, also known as Edge AI. Here, the data is processed (close) to where it is generated. At the 'edge' of a communication network or even without communication network. The aim is to minimise latency times and improve the efficiency of data processing by placing the AI software processing resources (e.g. embedded computing systems) closer to or directly at the devices that generate or use data (e.g. cameras). Well-known examples include autonomous driving, traffic detection and routing in smart cities or various applications in the context of Industry 4.0.

As the variants 2.-5. mentioned above are ultimately all hybrid approaches, we will focus on edge computing (variant 1.) in the following considerations.

Advantages of decentralised edge AI

Decentralised AI, more commonly known as Edge AI, offers several advantages over centralised systems:

1. **Data protection and security:** By distributing data processing across multiple nodes, the risk of data breaches is reduced. Sensitive data remains local and does not have to be sent to central servers, which reduces the risk of data theft. At the same time, the possibility of centrally compromising influence is reduced.
2. **Robustness and reliability:** Decentralised systems are less prone to failure as there is no single source of error. Even if one part of the system fails, the other parts can continue to function.
3. **Scalability:** Decentralised systems can be scaled more easily as new nodes can be added without overloading a central infrastructure. This enables more flexible adaptation to increasing requirements.
4. **Lower latency:** As processing takes place closer to the point of data acquisition, delays can be minimised. This is particularly important for real-time applications such as autonomous vehicles, Industry 4.0 or visual surveillance.
5. **Cost reduction:** Decentralised systems can be more cost-effective as they often require less central infrastructure and maintenance. In addition, existing local computing resources can be utilised to drive down the OPEX for AI significantly.
6. **Data sovereignty:** Organisations and individuals retain control over their data, which is particularly important in sensitive areas such as energy industry, defence sector, healthcare or personal data.
7. **Adaptability:** Decentralised systems can be more easily adapted to specific local requirements. Different regions or industries can make their own optimisations and adjustments.
8. **Innovation and competition:** Decentralisation promotes innovation as different players can work independently on solutions. This leads to a competitive environment in which new and improved technologies can emerge.

These advantages make decentralised AI an attractive option for many areas of application, especially where data protection, cyber security, scalability and reliability are of particular importance.

Robustness and reliability

With a particular focus on energy automation, especially the robustness and reliability required here, it should be noted that Edge AI can improve the robustness and reliability of artificial intelligence enabled solutions through several specific mechanisms:

1. Local data processing:
    - **Independence from network connections:** As data processing takes place locally, AI systems are less dependent on stable and fast Internet connections. This is particularly useful in remote or poorly Internet connected regions.
2. Distributed architecture:
    - **Fault tolerance:** By distributing data processing across many edge devices (embedded computing systems), the whole solution can continue to work even if individual devices fail or are impaired. This distribution increases fault tolerance and the robustness of the overall system.
    - **Load distribution:** The processing load can be distributed across multiple devices, reducing the likelihood of overloads and failures. This leads to a more stable and reliable performance.

    In the specific case of AI PowerBrain™ software from PowerBrain.Shop®, for example, one AI PowerBrain™ is installed per camera and per embedded system in order to ensure maximum robustness and fastest data processing.
3. Locally optimised models:
    - **Adaptation to local conditions:** AI models can be specifically adapted to local conditions and data on edge devices. This leads to more accurate and relevant results as the AI models applied are tailored to the specific requirements and environments.
    - **Continuous improvement:** Edge AI devices can continuously collect new data and improve models locally, leading to constant optimisation and adaptation of AI.

    This helps to improve quality assurance, for example, by comparing several data sources with each other through triangulation, to confirm an observed fault several times (e.g. with cameras from different angles) and thus minimise false alarms.
4. Energy efficiency:
    - **Local processing saves energy:** Reducing data traffic to central servers saves energy for long chains of communication infrastructure, as the data is processed locally. This can be particularly advantageous in environments with limited energy resources.
    - **Optimised resource usage:** Edge AI devices can use their energy and computing resources efficiently to run their AI models, resulting in overall more reliable and stable performance.

For example, the embedded systems that operate AI PowerBrains™ for optical video surveillance can automatically 'put to sleep' if there is no lighting at night and no additional lights in place, reducing their energy consumption at night. At the same time, those embedded systems that operate AI PowerBrains™ for thermal video surveillance can continue running, as they don't require day light for asset inspections.

5. Security and data protection:
    - **Less susceptibility to attacks:** By processing and storing data locally, edge AI devices are less susceptible to data breaches and attacks on centralized infrastructure such as a data centre, that could affect the availability and reliability of an entire AI solution globally.
6. Real-time monitoring and maintenance:
    - **Proactive fault detection:** Edge AI devices can be continuously monitored to detect and resolve potential faults or issues early and at one point or sensor, before they impact the whole system's performance and quality.

Through these approaches, edge computing of Edge AI can significantly improve the robustness and reliability of AI systems and solutions by reducing reliance on centralised resources and providing a more flexible, adaptable and cyber secure infrastructure.

Latency minimisation

From the operational perspective of an energy supply company (e.g. utility, DNO, DSO or TNO), detecting and reacting to problems in a substation as quickly as possible is crucial in order to minimise damage to people, systems, assets and power grids.

Edge computing can reduce the latency of artificial intelligence in several ways:

1. Local data processing:
    - **Direct processing at the point of data collection:** Processing data directly on the edge device where it is collected eliminates the need to send data to remote central servers and receive the results back. This significantly reduces latency.
    - **Real-time processing:** Edge devices can process data in real time, minimising delays and enabling quick AI decisions on site. This is particularly important for time-critical applications such as energy automation, autonomous vehicles, industrial control systems and health monitoring.
2. Reduced network dependency:
    - **Minimisation of data transmissions:** As large amounts of data do not need to be transferred over a communication network, the dependency on network bandwidth and quality is significantly reduced, as well as the latency caused by network congestion or slow connections.

3. Optimised Data Processing:
    - **Pre-processing of data:** Edge AI devices can pre-process data and only send relevant information to central servers and data centres, reducing the amount of data transferred and increasing efficiency. This speeds up and de-risks the entire data processing chain significantly.
4. Direct interaction and feedback:
    - **Local decision making:** Edge AI devices can make local decisions without having to wait for feedback from central servers or data centres. This is particularly useful in situations that require quick reactions, such as when processing sensor or video surveillance data at critical infrastructure such as substations, for example.
5. Intelligent data forwarding:
    - **Edge gateways:** Edge gateways could act as intermediaries, intelligently forwarding data and sending only the necessary information to central AI servers. This reduces latency by avoiding unnecessary data transmissions.
6. Optimisation of computing resources:
    - **Resource management:** Dynamic resource management on Edge AI devices can ensure that critical applications are prioritised and resources are used optimally, reducing processing time and latency.

Challenges in using decentralized Edge AI

Edge AI offers many advantages mentioned above. Special attention should be paid to some aspects when using it:

1. Limited computing resources:
    - **Limited hardware capacities:** Decentralised systems (edge computers) often have less computing power and storage capacity compared to centralised large-scale data centres, which limits the complexity and size of their AI models.
    - **Performance:** Training very large AI models on very large training data sets takes significantly longer on Edge AI computing systems compared to AI server farms.
2. Complexity of implementation:
    - **Distributed infrastructure:** The management and maintenance of a very large number of Edge AI devices may be inherently complex and should be addressed using specialised software update and maintenance tools as well as systematic processes.

3. Data synchronisation and consistency:
    - **Inconsistent data:** Ensuring data consistency and synchronisation across many decentralised devices could be a challenge. Different devices may use different versions of data and AI models.
    - **Synchronisation latency:** The time it takes to synchronise data or AI models between different Edge AI devices can lead to delays and inconsistencies.
4. Security risks:
    - **Vulnerable endpoints:** As many devices act as endpoints in a decentralised system, the number of potential points of attack increases. Therefore Edge AI device must be secured individually - which increases the reliability of the overall system.
      At the same time it also significantly increases the costs and effort for a potential cyber attacker.
    - **Physical security:** Edge AI computers or embedded systems are often located in less protected environments than central data centres, which makes them more susceptible to physical attacks. They should be stored and operated in correspondingly secure environments, e.g. within substation buildings or enclosed assets.
5. Limited data availability:
    - **Local data:** Edge AI devices only have local access to locally available data, which can limit the amount and variety of data available for training their AI models. They must therefore be equipped with additional training data sets if required, e.g. via time-limited data connections and remote access.
    - **Lack of a global view:** The decentralised nature of Edge AI can make it more difficult to obtain a comprehensive global view of all data. A regular exchange of any relevant data should therefore take place to help building AI models with a global perspective.
6. Network dependency:
    - **Connectivity issues:** Although Edge AI computing is designed to reduce dependency on central communication networks, many applications may still require occasionally some network connectivity for synchronisation, software updates and occasional data transfer. Unstable or slow connections can affect the speed of these transmissions.
    - **Data transfer costs:** The possible occasional synchronisation and data exchange between many edge devices and/or central systems can cause additional bandwidth costs.
7. Complexity in the management of AI models:
    - **Federated learning:** Although federated learning offers benefits, it is complex to implement and requires robust mechanisms for aggregation and synchronisation of AI model updates.

- **Model distribution:** Distributing and updating AI models across many Edge AI devices is complex and can lead to versioning issues. Therefore applying systematic configuration management processes is recommended.

Conclusion

The previous explanations show that decentralised Edge AI software architectures offer major advantages for time-critical and cyber secure applications. Especially in the energy industry they help fulfil the highest requirements for reliability and cyber security. In order to implement these Edge AI technologies successfully, well thought-out software design and careful management of the decentralised systems are required. The use of suitable software tools and systematic processes helps master Edge AI technology at the professional level and quality required by the energy industry globally.

The growing AI computing power and data storage capacity of decentralised embedded systems and Edge devices, together with falling market prices for them, helps rapidly spreading Edge AI applications across industries around the world. This development will continue to increase process efficiency and making processes more secure. By utilising the potential offered by Edge AI, you can create solutions that are up to the challenges of the future.

Authors

Mirko Düssel

Managing Director of Mirko Düssel & Co., a Strategy- and Marketing Consultancy in Kaarst, Germany.

E-Mail info@duessel.com
Web www.duessel.com

Samuel T. Stähle

CEO of PowerBrainShop Holding Corp., a Software technology supplier of „Plug and Play“ Edge Artificial Intelligence (B2B).

E-Mail samuel.staehle@powerbrain.shop
Web https://powerbrain.shop