

Cost-Effective IoT and OMS as the ‘Poor Man’s SCADA’

Author Peter Hellberg Co-founder & CIO of Acumen Software

acumen software

Contents

01 Abstract

01 Introduction

The MV and LV Network Challenge

03 Chapter 1

Evolution of Monitoring and Control in Electrical Distribution

05 Chapter 2

The Development of Smart Grids & Micro Grids

07 Chapter 3

IoT and OMS: The 'Poor Man's SCADA' Solution

13 Chapter 4

Key Communication Technologies for Enabling 'The Poor Man's SCADA'

16 Chapter 5

Edge Computing & Digital Twins

18 Chapter 6

Advantages of IoT and OMS Over Traditional SCADA

20 Chapter 7

The Future of MV and LV Network Monitoring and Control

22 Conclusion

The Future of MV and LV Network Monitoring and Control

23 Bibliography



Abstract

This white paper presents an intelligent approach to modernising medium-voltage (MV) and low-voltage (LV) electricity distribution networks through the integration of Internet of Things (IoT) devices and Outage Management Systems (OMS) as a scalable, sustainable alternative to traditional SCADA systems. Conventional SCADA solutions, while effective in transmission networks, remain costly, complex, and often impractical at these levels. In contrast, cost-effective IoT and OMS solutions, often described as the "Poor Man's SCADA", enable real-time monitoring, rapid fault detection, and advanced control without the costly investment and operational overhead of legacy systems.
The paper examines key enabling technologies including Low-Power Wide-Area Networks (LPWANs) for long-range communication, fault current indicators for precise fault localisation, and edge computing for low-latency processing and automation. Use cases and examples illustrate how these technologies improve reliability, response times and reduce maintenance costs. By enhancing real-time network visibility and supporting predictive maintenance, IoT and OMS solutions strengthen resilience and optimise asset performance. Ultimately, the paper recommends that utilities adopt these digital tools to drive efficiency, lower costs, and position their networks to meet future demands and competitive pressures. Through strategic implementation, utilities can build more adaptable, intelligent and sustainable power distribution infrastructure.

Introduction

The MV and LV Network Challenge

Medium voltage (MV) networks are defined as those operating between 1 kV and 35 kV, in accordance with the International Electrotechnical Commission (IEC) standard. They transport electricity from substations to transformer stations, supplying power to industries, hospitals, and urban areas. These networks, which can be overhead or underground, must adhere to strict safety requirements, including proper grounding, bonding, and insulation to ensure system stability and to prevent hazardous failures.

Despite its critical role in power distribution, the monitoring and management of MV networks remain a major challenge. These networks feature diverse topologies, requiring advanced protection systems such as earth fault protectors, circuit breakers, and reclosers to operate correctly.

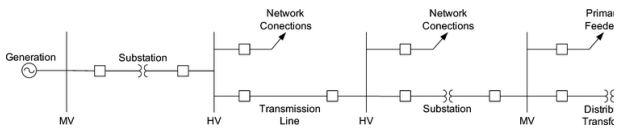


Figure 1: A typical power system scheme (Paulo et. al, 2014)

Additionally, maintaining stable voltage levels across MV networks is complex due to fluctuations in demand, variable load conditions, and the integration of distributed energy resources (DERs) such as solar and wind power. The need for

continuous monitoring and advanced control mechanisms is evident to maintain grid stability, efficiency, and resilience.

One of the primary challenges in MV networks is their geographical dispersion. Transformers and substations are often located far apart, necessitating long cable runs that lead to voltage drops and electrical losses. Traditional monitoring methods rely heavily on wired infrastructure, which is expensive, difficult to implement, and often lacks flexibility. The costs associated with installing and maintaining these systems often deter utilities from fully monitoring MV networks, resulting in blind spots in network visibility. In cases where faults occur in remote locations, the lack of real-time monitoring and automation means that utilities must rely on manual fault-finding processes, which are time-consuming and prone to human error. This results in longer outage durations, higher operational costs, and increased customer dissatisfaction.

Another concern is the impact of environmental and operational factors on MV network reliability. According to Rahardjo (2021), MV networks are prone to outages caused by both internal and external issues. Common issues include connection errors in underground cables, transformer malfunctions, and equipment wear and tear, while external threats such as thunderstorms and floods further exacerbate network instability. In the absence of a robust Outage Management System (OMS) and real-time monitoring capabilities, fault detection and isolation remains inefficient, leading to prolonged outages and higher maintenance costs.

Low voltage (LV) networks, which form the final stage of the electrical distribution system, face their own set of unique challenges. These networks supply power to homes and businesses, with transformers stepping down MV voltages to usable levels. LV networks are highly dynamic, experiencing fluctuations in demand due to varying load profiles and the growing insertion of bidirectional power flow from distributed energy sources, such as residential solar systems.

Due to each part of the LV network being shared by a much smaller number of customers compared to HV or MV infrastructure, the LV infrastructure cost must be minimised, hence it is seldom cost-effective to introduce real-time monitoring using traditional SCADA methods. This lack of telemetry leads to delayed outage responses, increased maintenance costs, and inefficient asset management.

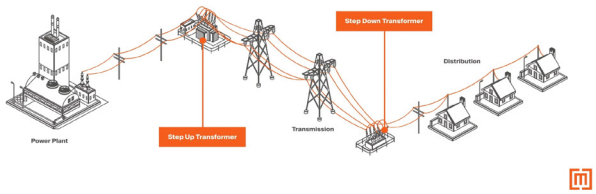


Figure 2: Voltage Step Up & Step Down-Transformers (Maddox, 2024)

The absence of advanced monitoring solutions forces utilities to operate reactively, addressing faults only after they are reported by customers, rather than employing predictive maintenance strategies. This results in higher operational expenses, longer restoration times, and greater network inefficiencies. The rapid adoption of electric vehicles (EVs), rooftop solar, and battery storage further complicates LV management, requiring more granular monitoring to balance loads and prevent voltage instability.

Traditional SCADA systems, while effective for monitoring high-voltage networks, are rarely implemented at the MV and LV levels due to their high costs, infrastructure requirements, and lack of scalability. These systems are designed for centralised control of large-scale power transmission but are often impractical for distributed, lower-voltage networks. As a result, many MV and LV networks operate with minimal real-time visibility, relying on manual inspections and post-fault analysis, which limits operational efficiency and increases the risk of prolonged outages.

The need for cost-effective, scalable solutions to address the shortcomings of MV and LV monitoring is clear. The integration of IoT-enabled sensors and intelligent Outage Management Systems (OMS) provides a valuable solution, allowing utilities to monitor, diagnose, and manage MV and LV networks in real time without the heavy capital investment required for traditional SCADA deployments. IoT-based monitoring solutions provide a flexible, wireless alternative, reducing the dependency on expensive wired infrastructure while enhancing fault detection, load balancing,

and network resilience.

As power distribution networks become increasingly complex, the demand for smarter, data-driven monitoring solutions is growing. The transition from traditional SCADA to IoT-enabled OMS solutions represents a shift in how utilities approach MV and LV network management. By harnessing real-time data, automation, and predictive analytics, utilities can achieve a more resilient, cost-efficient, and customer-centric grid.

01

Evolution of Monitoring and Control in Electrical Distribution

SCADA systems have played a pivotal role in electricity distribution monitoring since their introduction in the 1960s and 1970s.

These systems have evolved significantly over the decades, undergoing four distinct stages of development:

Monolithic SCADA Systems:

The earliest SCADA systems, known as monolithic SCADA, operated in isolated systems, relying on mainframe computers for data processing. Their lack of external connectivity made them highly secure, but they were rigid, expensive, and lacked scalability.

Distributed SCADA Systems:

By the 1980s, distributed SCADA systems emerged, introducing the ability to connect multiple processors via local area networks (LANs). This shift enabled greater flexibility, improved system reliability, and enhanced data sharing across multiple locations. Unlike their monolithic predecessors, these systems ensured that if one node failed, the overall system would continue to function.

Networked SCADA Systems:

The next significant advancement came in the 1990s with the introduction of networked SCADA systems, which leveraged wide-area networks (WANs) and the internet to enable remote monitoring – taking some semblance of SCADA systems as we know them today. This transition allowed for centralised control over large, complex operations, such as national power grids and industrial manufacturing facilities. The increased scalability and redundancy of networked SCADA made it the industry standard for power distribution management - though this came at a high price, with substantial implementation and runtime costs.

IoT-Integrated SCADA Systems:

In recent years, SCADA systems have entered a new phase with the integration of IoT technologies. IoT-enabled SCADA systems utilise internet-connected sensors and devices to collect vast amounts of real-time data across widely dispersed assets. Modern cryptographic methods have made it possible to transmit sensor data from low-cost sensors and actuators over public infrastructure securely, which is essential for mission-critical systems like power distribution networks. This evolution has introduced new capabilities, such as predictive maintenance, detailed performance analytics, and greater adaptability for MV and LV networks. The emergence of IoT-driven monitoring has now made it possible to extend SCADA-like functionalities to lower-voltage infrastructure at a

fraction of the cost.
Despite these advancements, many utilities still operate legacy SCADA systems, often adopting a "if it isn't broken, don't fix it" mindset. The reluctance to modernise is primarily driven by the significant investment required for both infrastructure and training, as well as by vendor lock-in to proprietary protocols and architectures. However, as electrical grids become more complex, and demand for real-time monitoring increases, utilities are beginning to recognise the long-term benefits of transitioning to more flexible, cost-effective

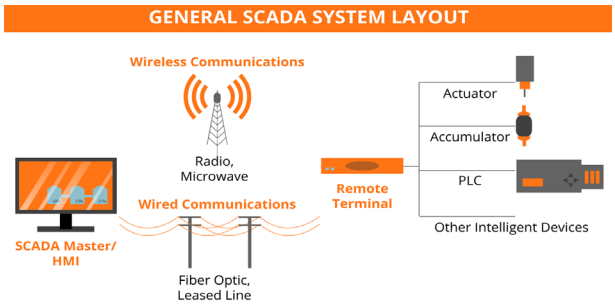


Figure 3: Diagram of a General SCADA System Layout (Deramsey, 2024).

solutions.

Key Advancements in the Past Two Decades:

Over the past twenty years, the monitoring and control of electrical distribution networks have undergone profound transformations. One of the most significant advancements has been the integration of IoT sensors into SCADA-based monitoring. IoT-enabled sensors allow for real-time data acquisition. Significantly improving fault detection, predictive maintenance, and remote diagnostics. Unlike traditional monitoring methods, which rely on periodic data collection, IoT-based monitoring ensures continuous visibility over network performance, reducing downtime and improving overall efficiency.

The introduction of edge computing has further enhanced SCADA capabilities by enabling distributed processing at the sensor level. This reduces reliance on central processing units and improves response times for critical grid operations. Instead of sending vast amounts of raw data to a central control system, edge computing allows preliminary data processing to occur at the device level, reducing latency and improving overall system performance.

Another major development has been the transition from traditional wired SCADA to wireless and cloud-based systems. The adoption of 4G LTE, 5G, LoRaWAN, and NB-IoT has allowed utilities to deploy SCADA systems in remote and geographically dispersed areas without the need for costly wired infrastructure. Cloud-based SCADA solutions further support scalability, enabling utilities to centralise data collection while reducing software licensing and hardware maintenance costs.

The integration of SCADA systems with OMS has also been a key milestone in modern power distribution management. The ability to leverage real-time SCADA data within OMS platforms has enabled automated Fault Detection, Isolation, and Service Restoration (FDIR), significantly reducing outage response times and improving grid resilience. With access to real-time outage data, utilities can pinpoint fault locations, predict outage impact, and optimise restoration strategies more effectively.

Advancements in artificial intelligence and machine learning have further optimised SCADA operations. AI-powered algorithms are now capable of improving load forecasting, demand response, and failure prediction. By analysing historical trends and real-time grid conditions, AI can identify patterns that indicate potential faults, allowing utilities to take preventative action before disruptions occur. These innovations are making SCADA systems not only more efficient but also more proactive in maintaining grid stability.

The transition to IoT-enabled SCADA solutions presents a shift in how MV and LV networks are monitored and managed. IoT-enabled solutions eliminate the need for expensive hardwired infrastructure, reducing both capital investment and operational costs. Additionally, the increased granularity of data provided by IoT sensors allows for better predictive maintenance, dynamic load balancing, and automated fault detection, resulting in a more resilient, efficient, and responsive distribution grid.

SCADA and IoT technologies are not necessarily competing solutions; instead, they can be leveraged together to maximise their strengths. Traditional SCADA systems provide reliability and robustness, while IoT introduces flexibility, scalability, and cost efficiency. A hybrid approach allows utilities to take advantage of SCADA's reliability while benefiting from the enhanced data insights and remote accessibility that IoT offers. Heisenware (2025) illustrates this complementary relationship through the example of remote production facility monitoring, where SCADA is used to control on-site machinery, while IoT platforms transmit collected data to the cloud for further analysis. This model demonstrates how combining SCADA and IoT can provide utilities with deeper insights and more effective control strategies, ultimately improving the efficiency.

02

The Development of Smart Grids & Micro Grids

The Development of Smart Grids & Micro Grids
Energy sustainability and environmental preservation have become global concerns - making the need for affordable, advanced, and sustainable energy solutions increasingly urgent. Tuballa & Abundo (2016, p. 710) note that if electricity consumption continues to rise unchecked, it may become unmanageable.

As cities and nations grow and become more technologically advanced, solutions such as Smart Grids and Microgrids, often powered by IoT technologies, have emerged to modernise and strengthen energy infrastructure.

The evolution of Smart Grids can be traced back to the early 2000s, these grids were simplistic, with a primary focus on improving grid efficiency and reliability. By the 2010s, greater focus was placed on sustainability and the integration of renewable energy sources. The development of Advanced Metering Infrastructure (AMI) played a significant role during this period, as did the growing deployment of IoT devices and smart meters.

In the 2020s, the incorporation of AI and machine learning technologies further advanced Smart Grids, alongside increasing emphasis on edge computing and cybersecurity. These developments have made Smart Grids more autonomous, enabling utilities to optimise existing infrastructure and reduce the need for new power plants and substations (Tuballa & Abundo, 2016, p. 711).

Smart Grid pilot projects have been increasingly, and successfully, implemented across both developed and developing nations, offering a more sustainable, efficient, and affordable approach to electricity distribution.

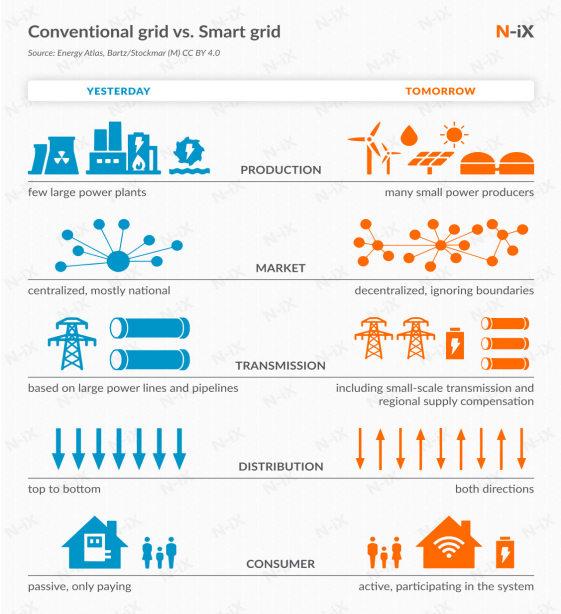


Figure 4: Conventional Grid vs. a Smart Grid (Ni-X, 2023)

For instance, in 2009, Spain became one of the first countries to convert its national grid into a Smart Grid. Over 10 million smart meters were installed throughout the country before the end of 2018. This mandatory rollout proved beneficial not only for consumers but also for the broader economy. Smart Energy International (2016) estimated that Smart Grids could generate over 200,000 jobs in Spain and help position the country as a leader in the global technology sector.

India also implemented their own Smart Grid pilot project known as the Puducherry Pilot Project, which officially commenced in 2012. Despite initial setbacks due to funding challenges, the project was completed in 2016 and was considered a success. It significantly improved the efficiency and reliability of the distribution network, enabling

near real-time monitoring and responsive supply-demand balancing. Both consumers and utilities benefited: users could track and adjust consumption, while the utility improved outage management and operational efficiency.

Kappagantu et al. (2015, pg. 99) highlight that despite the project's success, there were five major challenges faced during implementation:

1. Interoperability: Since Smart Grid components are developed by various manufacturers worldwide, it is vital that systems adhere to common standards. Without standardisation, compatibility issues may arise.

2. Cybersecurity: Smart grids use digital technologies to monitor, control, and exchange data across different parts of the power system. This makes them more efficient but also more vulnerable to cyber threats, like hacking or malware, and physical tampering. To ensure safe operation and to maintain trust, the system must be built to block these threats and safeguard customer data.

3. Communication Technologies: Smart grids rely on various communication methods, but challenges like cost, reliability, and technical interference must be addressed to ensure consistent performance.

4. Social Barriers: For Smart Grid programs to be successful, the end-users needs to participate in the projects. Awareness programs clearly explaining the benefits are necessary to encourage proactive participation.

5. Political Barriers: The high upfront cost of implementing smart grids can create hesitation among administrators, policymakers, and project leaders. They need to be convinced of the long-term benefits and return on investment, especially given the potential for temporary disruptions to electricity supply during the rollout.

These barriers highlight the complexity of upgrading traditional power infrastructure to meet the demands of a smarter, more efficient grid. As these issues continue to be addressed, attention is also turning towards **microgrids** - smaller, decentralised energy systems that offer greater flexibility, resilience, and localised control.

According to Eskom, South Africa's primary electricity provider, Microgrids are defined as collections of interconnected loads and distributed energy resources (DERs) that function as single controllable entities within clear electrical boundaries. They can operate independently or be grid-tied, maintaining stable power quality parameters even when disconnected from the national grid.

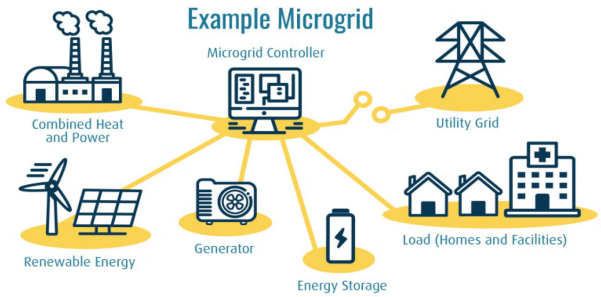


Figure 5: Example Microgrid Diagram (San Miguel Power Association, 2023)

In a 2019 study, The World Economic Forum estimated that there were approximately 4500 microgrid projects worldwide. These systems are particularly valuable in emergency situations, such as during storms when the main grid is disrupted. Eskom also identifies microgrids as a viable solution for remote or hard-to-reach communities, where traditional grid connection is economically or logistically unfeasible, as well as for areas facing network capacity constraints.
Microgrids generate and store their own energy, oftentimes making use of renewable energy – such as wind turbines or solar panels, meaning that microgrids can help reduce greenhouse gas emissions. The International Energy Agency (2024) considers microgrids the most affordable means for extending electricity access in developing countries.

Eskom has established two successful microgrid pilot sites. Ficksburg Microgrid in the Free State, which supplies electricity to over 10 households, and Lynedoch Microgrid in the Western Cape, which interconnects over 30. These projects have demonstrated that a cleaner alternative to conventional grid supply is indeed possible. Eskom states that the implementation of microgrids also uplifts the community. By leveraging local labour and resources, they support community empowerment and economic growth. As Behere (2024) observes:

This technology facilitates the transition towards smarter, cost-efficient and more resilient grids, aligning with the goals of urban utilities to modernize their infrastructure to meet the evolving needs of urban populations. Utilities can improve service quality, minimize disruptions, and lay the foundation or future grid advancements and innovations.

This growing integration of smart and decentralised infrastructure points to the need for adaptable digital systems, ones that can bring real-time visibility, control, and optimisation to resource-constrained and remote environments. It is within this context that IoT and OMS technologies emerge as powerful enablers - forming the backbone of what is now known as the 'Poor Man's SCADA' system.

03

IoT and OMS: The 'Poor Man's SCADA' Solution

IoT and OMS: The 'Poor Man's SCADA' Solution
IoT technology is increasingly being deployed across electricity distribution networks to enhance visibility, control, and automation, particularly in medium and low voltage systems.

IoT sensors, actuators, and gateways are fundamental for real-time monitoring in MV and LV networks. These components work together to collect, process, and act on data, ensuring grid stability, automation, and fault detection. They are essential for efficient power distribution, rapid fault response, and predictive maintenance.
To understand the current role of IoT-driven telemetry, we must first explore the evolution of sensors in power systems.

Sensors have long played a crucial role in network monitoring. Swain et al. (2022) highlight the importance of understanding the history and evolution of sensors, not only for contextualising today's innovations, but also for guiding future advancements. The evolution of sensors in power systems can be divided into four major phases:

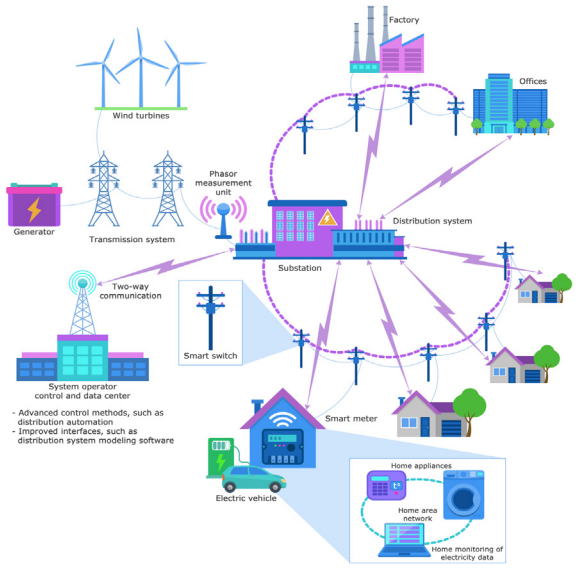


Figure 6: Smart Grid Diagram (CS Odessa, n.d)

Phase 1: The Inception Phase (1880s–1900s)
The inception phase represented the early deployment of instruments to measure basic grid

and atmospheric parameters, using rudimentary devices to monitor grid currents. According to Elliott (1991), there were reports in the 1890s of the first remote sensing device - the "radiosonde." This telemetry instrument, typically carried by a weather balloon, measured various atmospheric parameters. Early sensors in power networks were bulky and primarily installed on transformers, measuring voltage and current.

Phase 2: The Growth Phase (1900s–1950s)
This phase marked an increasing recognition of the importance of measuring devices for grid monitoring and protection. By the late 1950s, technological advancements had led to more versatile sensors, which could detect new fault indicators such as temperature, acoustics, pressure, chemical changes, and gas composition (Swain et al., 2022).

Phase 3: The Digitalisation Phase (1960s–1980s)
As power grids became more complex and operated at higher loads, sensors needed to be faster and able to measure multiple grid components. The development of semiconductors, paired with the fabrication of system-on-chip devices paved the way for high performance but low-powered, lightweight sensors, replacing their bulky predecessors. These advancements made it possible for sensors to be installed remotely and increased the visibility of the grid components. The 1970s also saw the invention of SCADA systems.

This facilitated the deployment of monitoring instruments and sensors that had faster response times and that could initiate local protective actions such as the action of circuit breakers, reclosers, and isolators. However, these sensors had lower sampling rates that were insufficient in the detection of details of transient phenomena that occurred in mere milliseconds. To capture this underlying data for optimum asset utilisation, fast acting sensors and switches were deployed in the late 1980s (Swain et al., 2022).

Phase 4: Smart System Integration (1990s–Present)
The current phase of sensor development is characterised by smart system integration. The introduction of Microelectromechanical System (MEMS) technology in the 1990s improved sensor accuracy, followed by real-time monitoring sensors in the 2000s that integrated with PMUs (Phasor Measurement Units) and SCADA systems.

Today, utilities demand real-time data from SCADA and PMU-based systems for Dynamic Security Assessment (DSA), predictive controls, and system modelling. To transition into smart grids, power systems require instantaneous, high-accuracy, and synchronised sensing. Smart sensors, Wireless Sensor Networks, and AI-driven telemetry are transforming power grids - enhancing automation, fault detection, system protection, and real-time grid stability.

IoT Sensors in MV and LV Networks
IoT sensors are responsible for real-time data collection across MV and LV networks, continuously monitoring key electrical and environmental parameters. There are a wide range of IoT sensors available, including pressure sensors, temperature sensors and voltage sensors. The sensor-gathered data is analysed, traditionally by a SCADA system, before the actuators execute the decision made from the analysis. For example, a pressure sensor detects a pipeline issue, the SCADA system would then determine if action needs to be taken, in this case, it will decide pressure needs to be reduced. Lastly, the actuator will then execute this by opening a valve to release pressure.

Some of their other key roles include power quality and harmonics analysis – to identify abnormal disturbances and to maintain grid reliability.
IoT sensors enable real-time decision making, providing utilities with instant insights into grid power conditions. They also support automated fault response to minimise downtime, as well as reducing the need for frequent manual inspections.

IoT sensors revolutionise MV and LV network operations by enabling real-time monitoring, predictive maintenance, and automated responses. Their role in fault detection, load optimisation, safety monitoring, and DER (Distributed Energy Resource) integration makes them indispensable for modern power distribution systems.

A practical example of this can be seen in Delhi, India, where Tata Power-Delhi Distribution implemented one of the first large scale IoT infrastructures in LV network distribution, across 300 substations, from 2020 to 2022. The IoT project reduced fault restoration times by 41%, enabling faster service recovery after outages and leading to a 14.77% drop in customer complaints.

In a conference paper on this project, Behera (2024) notes that this project produced "inspiring results" and that the technology was reliable, easy to deploy and adaptable. Behera further advocates for the adoption of IoT-based LV automation by other utilities, emphasising the clear advantages over legacy systems.
This case reinforces the value of integrating IoT sensors in LV networks, showing that even under pressure from rapid urbanisation, digital solutions can deliver tangible improvements in visibility, reliability, and efficiency.

Actuators

Actuators create physical effects based on received electrical or digital control signals.

Thakker (2024) notes that these physical effects are typically motion or force, Thakker goes on to explain that these systems create a loop between the physical and digital world, enabling interaction and control. Actuators come in various types, such as mechanical, electrical and electromagnetic. Within each type of actuator, there are also a wide range of devices. For example, levers and hand cranks can be classed as mechanical actuators, whereas diodes and bipolar transistors can be classed as electrical actuators.

In MV and LV networks, actuators are responsible for automating switching, load balancing, fault isolation, and voltage regulation. Improving grid response times and reducing the need for manual intervention.
Despite their generally robust design, actuators are not immune to failure. Tameson (2023) highlights that excessive loading, or inadequate maintenance can lead to malfunctions, which, in worst-case scenarios, could result in total grid failure. Mitigation strategies such as redundancy, surge protection, and predictive maintenance are critical for maintaining grid stability.

IoT Gateways

IoT gateways act as communication bridges in MV and LV networks, ensuring seamless data transmission, processing and integration between IoT sensors, actuators and control systems. In simple terms, a gateway can be described as a combination of a router and a modem.

Gateways collect the real-time data from IoT sensors, such as voltage or current measurements, they then process and filter this sensor data. After this, protocol translation occurs to ensure compatibility between devices. Edge computing may occur, analysing the data locally to reduce dependency on cloud-based processing. The data is then encrypted and securely transmitted to either SCADA systems or cloud-based platforms. IoT gateways also feature failover mechanisms that automatically switch to backup networks in case of failure, ensuring continuous monitoring.

IoT sensors, actuators, and gateways are all vital for improving grid efficiency by ensuring real-time monitoring, data processing, transmission, and executing automatic responses. Benefits also include faster fault detection and isolation, improved grid resilience and stability, and efficient predictive maintenance, all while reducing downtime.

Integration of AMI in MV and LV networks

AMI (Advanced Metering Infrastructure), as defined by IBM, is an integrated, fixed network system, enabling two-way communication between utilities and customers. The data collected by the system provides utility companies with real-time monitoring capabilities across electricity, gas, and water systems, facilitating energy monitoring, balancing, and optimisation.

The most important component of AMI systems are smart meters that record energy consumption. This includes electric meters, digital gas meters and water meters. According to IBM, these meters typically send data back to utility companies at least once a day.

AMI networks also allow utility companies to send commands to meters, enabling remote meter management. This not only eliminates the need for manual meter readings but also enables faster response times in the event of a power outage. AMI systems include communication networks, data management systems, and analytics platforms that support monitoring, control, and optimisation. Some of the primary AMI applications in IoT-driven telemetry include real-time data collection, energy balancing, voltage and power quality monitoring, and secure, efficient energy transactions.

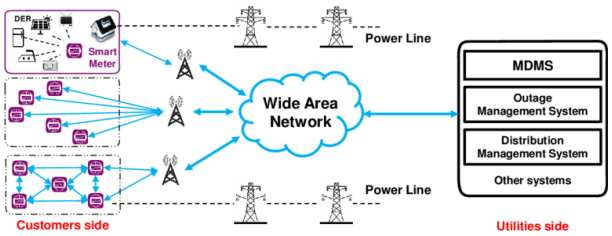


Figure 7: Basic Components of an AMI System (Derhab et. al, 2018)

AMI for Energy Balancing in MV and LV Networks

AMI supports real-time load monitoring and adjustment. For example, if an LV feeder is overloaded, AMI data helps redistribute power. In demand response and load-shifting scenarios, consumers with smart appliances can receive automated signals to reduce consumption during peak demand periods. Additionally, AMI manages fluctuations from Distributed Energy Resources (DERs), ensuring that if a DER exceeds demand in an LV network, AMI can trigger actuators to adjust outputs accordingly. Eskom, South Africa's primary electricity supplier, has executed pilot projects using smart meters for "load limiting" to prevent the need for rotational load shedding.

AMI for Theft Detection

AMI compares metered consumption to actual energy supplied and any anomalies, losses, or unauthorized connections are flagged

immediately. In South Africa, as well as throughout the developing world, illegal connections pose a significant challenge, contributing to overloaded grids, prolonged outages and financial losses that can threaten the viability of the entire utility. If a household reported low consumption but sensor data reflects high load flow, this could indicate tampering, which could be immediately actioned. By splitting the smart meter's user panel from the metering sensors and circuit breakers, the utility can cut off supply to the customer when tampering is detected and increase the difficulty of future meter circumvention.

AMI can also detect tampering and issue unauthorised access alerts. Smart meters come with tamper sensors and attempts to bypass metering can trigger real-time alerts to power utilities. Utilities could then remotely disconnect power from non-compliant consumers, and the AMI system could automatically generate fines accordingly.

DTMs

DTMs (Distribution Transformer Monitors) are IoT devices installed at distribution transformers to monitor voltage, load, and other key parameters. They also enable real-time monitoring and data transmission and can be deployed in MV and LV networks to provide cost-effective alternatives to traditional telemetry devices. They can detect issues such as voltage irregularity and power theft. In a trial performed by Network Waitaki (2018), they noted the benefits of DTM on LV networks, such as high-resolution granular data, enhanced visibility of transformer utilisation (under/overuse), improved capital renewal planning through accurate asset performance data, as well as better understanding of LV network behaviour with insights extending into MV networks.
DTMs help maintain grid stability by ensuring efficient energy distribution and minimising power theft, making them essential for modern smart grid management. Exciting work is also being done in terms of integrating DTMs with DERs and flexible loads, such as EV chargers and electric heating, to automatically balance loads at the distribution transformer scale.

Check Meters

Check meters are an essential secondary electricity meter installed alongside the main meters to cross-check energy consumption readings for accuracy and monitoring purposes. Their integration with IoT networks makes them vital tools for enhanced theft detection and load balancing.

Check meters are used in conjunction with AMI and DTM systems. IoT enabled check meters send alerts to utilities when anomalies are detected. Their integration with IoT telemetry systems enables predictive maintenance by detecting issues before failure occurs – their wireless communication support allows for remote monitoring with real-time data transmission. Whilst sharing some features with main meters, check meters are designed to ensure accuracy and verification, rather than measuring overall usage.

Check meters connected to IoT gateways can detect energy theft in real-time and through integration with the OMS or WMS (Work Management System) incorporate the response to energy theft events into day-to-day utility operations.

Benefits of IoT-based telemetry:

IoT-based telemetry in MV and LV networks enables real-time monitoring, automation, and intelligent decision-making, significantly improving grid efficiency, reliability, and security. Rugged Telemetry (2024) list 3 of the main benefits of IoT-based telemetry:

1. Real-time monitoring: Due to devices providing a continuous stream of real-time data, stakeholders can gain immediate visibility into energy usage patterns.

2. Data Analysing: Advanced analytics provide a deeper understanding of energy consumption patterns to help make informed decisions.

3. Automation & Control: Smart devices can be programmed to adjust settings based on real-time data – no manual intervention is required, ensuring efficiency and responsiveness.

There are a wide range of benefits to using IoT-based telemetry in MV and LV networks. Scalability and cost-efficiency being the primary benefits to traditional and expensive monitoring methods.

IoT-Based Control Systems:

Remote monitoring and control is an important issue for power management. Management is usually handled manually, or with expensive SCADA systems. Hossain et al. (2019) argues that reliable control over the entire sub-station can be achieved through introducing IoT technology.

> The IoT based system allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems and resulting in improved efficiency, accuracy and economic benefit with the added merits of minimum human intervention.

In medium voltage networks, motorised switchgears and remote-operated breakers can

be utilised for fault bypassing and remote service restoration, reducing the need for on-site visits.

Switchgear & Breakers

Switchgear control and protect electrical equipment. Switchgear contain fuses, switches and other power conductors. Schneider Electric (n.d.) note that circuit breakers are the most common component found in switchgear. If there is an electrical fault, the circuit breaker senses the anomaly and interrupts the power flow to limit damage to the system. Switchgear enhances safety and protects network equipment by preventing overloads and short circuits.
The key difference between motorised circuit breakers and standard circuit breakers is that motorised circuit breakers can be operated remotely and automatically. This remote functionality allows for real-time monitoring and control, enabling operators to respond quickly to faults, optimise system performance and reduce downtime. Motorised breakers provide enhanced security, improved efficiency, remote control and automation, durability and reliability, integration capabilities, and optimised maintenance. Given their versatility, the use of motorised breakers is expected to increase as electrical systems become more complex.

Remote-operated breakers eliminate the need for long cable runs, enabling the connection of geographically dispersed facilities. They also enhance worker safety by reducing the risks associated with arc flash incidents, as tasks can be performed remotely without direct exposure to electrical hazards.

Low Voltage Control Systems

Whilst low voltage remote control remains somewhat limited, IoT devices can still be used for things such as outgoing signals and localised control. Breaker status can be monitored in real time and phase-specific failures can be monitored. Smart switches, relays, and low-cost PLCs (Programmable Logic Controllers) provide affordable and effective control mechanisms for low-voltage systems.

Smart Switches

A smart switch in IoT-based electrical control systems enhances automation, fault management, load balancing, and grid efficiency. It provides remote, real-time control over electrical circuits, making modern power networks more intelligent, responsive, and resilient.

Relays

Relays are control and protection device in electrical systems, used to detect faults, automate switching, and improve grid reliability. Relays automatically open or close circuits in response to electrical signals. IoT-enabled smart relays communicate with SCADA, AMI, and IoT-based telemetry systems to support remote monitoring, data logging, and predictive maintenance.

PLC (Programmable Logic Controller)

PLCs are industrial computers used to control and monitor equipment, based on custom programming. Given the range of sizes and configurations, they can be adapted for various applications. They can be modular or fixed, with modular PLCs offering greater flexibility and memory. Fixed PLCs are smaller, more affordable, and include a predetermined number of inputs and outputs.

According to Inductive Automation (2020) many modern PLCs employ publish-subscribe protocols to combat cellular network costs for data transmission to ensure data collection is streamlined and occurs in real-time.

Long-life Battery Options

While traditional telemetry infrastructure has relied on grid-connected power supplies, the integration of self-contained, battery-powered IoT sensors presents a compelling alternative. This approach can dramatically reduce costs. Network monitoring typically occurs at MV levels and higher, necessitating dedicated transformers to power traditional SCADA equipment - adding costs, complexity and maintenance overhead. Utilising low-power IoT devices with dedicated batteries simplifies installations, enabling monitoring options that were historically too expensive, such as detecting fuse states on MV lines.

Traditional Centralised SCADA vs Decentralised Control for MV and LV Systems

In centralised control, a single control system, such as a SCADA system, oversees and manages the entire MV or LV network. Data is processed at this central location, and all decisions are executed from there.

This traditional approach has a slower response time when it comes to fault detection due to its reliance on central processing. Furthermore, if the control centre is down, the entire network may be affected. Traditional SCADA systems also have limited scalability, adding new devices increases system complexity and costs. The monolithic nature of SCADA systems creates limitations for data capacity and data transformation capabilities. TechTarget (n.d) notes that integration difficulties often lead to data and processing siloes, preventing SCADA systems from achieving high levels of interoperability.

SCADA systems are also highly vulnerable to cyber-attacks. Claroty (2024) highlights that one of the biggest cybersecurity challenges for SCADA systems is the lack of modern security features such as encryption and authentication.

By comparison, decentralised control, otherwise known as the IoT-based approach, distributes decision-making across multiple edge devices that operate autonomously or in coordination with control units.

Decentralised control offers faster response time, higher system resilience (failure of one control node doesn't impact the entire network), better integration which allows for better optimisation of energy, greater scalability and flexibility, making it ideal for smart grids and DERs.

A unique difference between IoT-based sensors and traditional SCADA telemetry is that modern IoT sensors can cheaply incorporate GPS sensors to report their position together with their sensor data. This allows IoT sensor data to be useful for operational purposes, even when they are not correctly "wired" into the SCADA network data schematic, greatly simplifying the rollout.

While initial implementation costs for decentralised control may be high, factors such as the cost-efficiency of cloud solutions and open-source technologies help reduce expenses.

Rather than forcing a choice between centralised SCADA and decentralised IoT-based control, Heisenware (2025) suggests that SCADA and IoT can complement one another. SCADA systems can be used for critical process control, while IoT technologies handle data analysis and remote monitoring. This approach combines SCADA's reliability with IoT's flexibility.

Nonetheless, decentralised control systems still provide a faster, more cost-effective solution for MV and LV networks compared to traditional centralised systems.

OMS as the Core Platform

OMS (Outage Management Systems) help electric utilities locate, analyse and fix power outages on the grid. An OMS can coordinate with multiple different data sources in order to process data from across the grid.

By integrating OMS with IoT-based telemetry, utilities enable intelligent FLISR capabilities, improving fault response, isolation, and service restoration in MV and LV networks. This leads to faster outage recovery, lower operational costs, and enhanced grid reliability.

In MV distribution systems, OMS identifies faults quickly and accurately through real-time monitoring of network conditions. OMS also analyses fault data from multiple sensors and smart meters to determine the exact fault location. Smart switches and circuit breakers communicate with OMS to isolate the faulty section and reroute power from alternate feeders and limits the areas affected by blackouts.

OMS also helps to balance electrical loads across MV networks. The real-time monitoring allows data collection to measure power demands on transformers and substations; smart switches and automated circuit breakers can shift the loads as needed. OMS also ensures that power distribution aligns with real-time demand fluctuations.

In the LV network, OMS integration allows for early-stage warning signs to be monitored – such as signs of failure and voltage imbalances. This integration enhances predictive maintenance, grid stability, and service reliability.

Due to OMS systems managing outages spatially, they can make use of data from IoT sensors that are not correctly allocated to devices in the network model based only on their GPS position.

Machine learning algorithms within OMS can analyse trends to detect abnormal conditions. For example, if an LV distribution transformer exhibits gradual overheating, OMS flags it for preventive maintenance before failure occurs. Smart meters and IoT-based check meters measure real-time load demand across LV feeders, allowing OMS to detect overloading trends and reallocate power to prevent system failures.

OMS with IoT sensors can also help maintain balanced voltage levels. Voltage sensors and smart meters continuously track phase voltages at LV transformers and feeders. OMS detects voltage deviations and fluctuations, sending alerts to utility operators. Voltage imbalances can cause motor overheating, reduced efficiency, and power losses for industrial and commercial consumers. OMS can notify large customers to take corrective action before disruptions occur, helping them avoid downtime and financial losses while maintaining overall customer satisfaction.

IoT-based outage detection reduces restoration times through automation, improves service reliability through real-time detection, enables predictive maintenance, facilitates remote monitoring, and enhances grid reliability metrics. Fewer outages and faster restorations improve SAIDI and SAIFI reliability indices, ensuring consumers experience less disruption. IoT-based outage detection transforms power grids into proactive, self-healing networks, improving resilience and efficiency.

04

Key Communication Technologies for Enabling 'The Poor Man's SCADA'

Key Communication Technologies for Enabling 'The Poor Man's SCADA'

Communication technologies play a critical role in enabling the data exchange that underpins the 'Poor Man's SCADA' solution. To support the real-time monitoring and control required by IoT devices, various cost-effective networking options have emerged - including LPWANs (Low-Power Wide-Area Networks), 4G/5G cellular networks, and mesh networks. These technologies are selected based on deployment scale, power constraints, and data transmission requirements, offering different trade-offs between cost, range, and control.

LPWANs

LPWANs are wireless communication networks designed for long-range connectivity with low power consumption, making them highly suitable for IoT applications. It includes technology such as LoRaWAN, NB-IoT and LTE-M. Depending on the technology, LPWANs can range between 30km to 100km (Velos, 2024). The reduced maximum output power allows devices to run on small batteries for as long as ten years in some cases. Since simple IoT devices do not stream large quantities of data to a server, LPWANs can efficiently accommodate and optimise the data transmission.

LoRaWAN

LoRaWAN utilises radio technology, specifically LoRa, to achieve long-range, low-power wireless communication. It enables communication between end-node devices and network gateways, supporting numerous sensors on a single gateway, making it a scalable solution. Its use of ISM (Industrial, Scientific, and Medical) bands means that users do not need to purchase expensive licences or pay network operators to operate their devices.

However, LoRaWAN can sometimes experience reliability issues, such as interference or data transmission delays. These challenges can typically be mitigated by deploying additional gateways and adjusting spreading factors to improve network performance.

NB-IoT

Narrowband IoT, also a radio technology, is designed for IoT applications requiring long-range, low-power, and deep indoor coverage, it provides reliable connectivity in hard-to-reach areas by effectively penetrating walls, basements, and other obstacles.

Optimised for IoT within cellular networks, NB-IoT relies on simple waveforms for connectivity and uses less power than LTE technologies. However, this results in a limitation on the amount of data it can transmit. Despite this, NB-IoT offers a cost-effective, simple, yet reliable means of real-time monitoring and control for MV and LV networks.

4G/5G Networks

4G and 5G networks are both mobile communication technologies. While they share similarities, 5G networks offer increased download speeds, even lower latency, and the capacity to connect a significantly larger number of devices without overwhelming the network. These networks are primarily used for mobile phones, broadband internet, and IoT devices.

One major advantage of mobile networks is their mobility, allowing users and devices to move between towers without losing connectivity - an edge over LPWANs, which have limited mobility. However, they tend to have shorter battery life compared to LPWAN technologies.

Although 5G technology is more advanced, 4G networks currently offer broader coverage due to existing cell tower infrastructure. As a result, 4G is considered the backbone of many modern

industrial applications. Both networks are strong enablers of speed, coverage, mobility support, and real-time data collection and control. It is likely that there will be a gradual shift from 4G to 5G as the technology becomes more widely adopted.

Mesh Networks

A mesh network is a local area network in which the infrastructure nodes (i.e. bridges, switches, and other infrastructure devices) connect directly, dynamically and non-hierarchically to as many other nodes as possible and co-operate with one another to efficiently route data (Zenarmor, 2022).

Mesh networks offer scalability, flexibility, robustness, security and reliability. They utilise radio technology for wireless communication and to create a decentralised structure. Mesh networks are self-healing networks, meaning that mesh networks have the ability to identify and rectify faults or problems automatically, without human intervention. Mesh networks are extremely useful for distributed and low power devices.

Mesh networks also offer reduced infrastructure costs, as they require fewer gateways and do not need extensive cabling. However, they are not well suited for high-speed network demands; in such cases, 4G/5G networks would be a more suitable option. Nonetheless, mesh networks remain a cost-effective alternative for large-scale IoT deployments where ultra-high speeds are not a primary requirement.

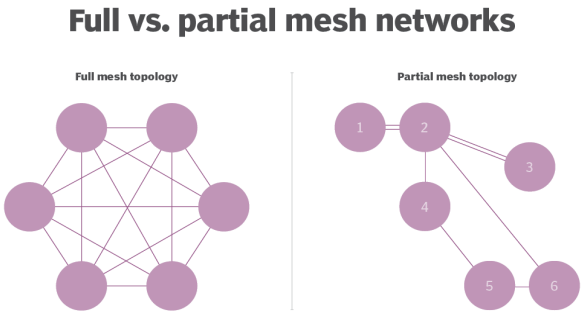


Figure 8: Full vs Partial Mesh Networks (Tech Target, n.d)

Importance of Redundant Communication Options

Reliable communication is a cornerstone of any functional SCADA system, ensuring that monitoring, control, and automation within MV and LV networks remain operational, even in the event of primary network failures. Redundant communication options mitigate single points of failure, improve grid resilience, and ensure continuous data flow. While cost-effective IoT-driven solutions such as LPWANs, 4G/5G networks, and mesh networks offer accessible alternatives to traditional SCADA communication, no single technology can provide 100% uptime. This is where redundant communication options become critical.

Network redundancy helps keep business operations running smoothly in the event of a failure. It also plays a key role in risk management and cost savings - both in terms of downtime costs and potential revenue loss caused by network outages. Redundancy ensures performance optimisation by balancing network traffic to prevent overloads. It also allows networks to handle growth and increased demand. In the event of major failures or disasters, redundancy enables quick network recovery. Additionally, redundancy is crucial for maintaining customer satisfaction by ensuring reliable services.

The type of network backup is determined by the requirements of the system. For example, if 4G/5G is being used as the primary communication technology, LPWANs could be used as the redundant backup. If a 4G tower goes down during a storm, LoRaWAN-enabled sensors could continue transmitting outage data. Even field-technicians require a redundant backup. If a technician was working on a MV fault in a remote location using 4G, but the cellular service become unavailable, a satellite link could be used to provide an emergency backup.

A cost-effective 'Poor Man's SCADA' system must leverage redundant IoT-driven communication technologies. The right blend of LPWAN, cellular, fibre, and even satellite ensures that even the most budget-conscious utilities can achieve real-time control and automation without relying on expensive traditional SCADA systems.

Open-Source and Cloud Solutions

Open-Source SCADA systems are software-based systems that provide full access to the source code, allowing utilities, developers and engineers to modify and customise the functionality according to their specific needs. It encourages open collaboration, as well as transparency and security. Aghenta, L & Iqbal, M. T (2021) refer to open-source SCADA as being a "mix and match" system. Open-source SCADA systems integrated with IoT offer increased flexibility.

No single supplier is responsible for overall system performance, which significantly reduces user vulnerability. This makes open-source systems a more cost-effective solution, as users are not locked into using a single, potentially expensive, supplier. Should a supplier go out of business or experience other issues, system components can be replaced with similar alternatives from different manufacturers, offering much greater adaptability

than traditional SCADA systems.

SCADA in the Cloud

Cloud-based SCADA software enables organisations to monitor and control their processes remotely, rather than relying on on-premise hardware. These platforms allow for advanced, real-time data analysis, enabling automated decision-making. The accessibility of cloud-hosted data introduces greater flexibility in both personnel and resource management. Streamlining data collection through cloud-based SCADA optimises operations, facilitates preventative maintenance, and improves the ability to identify emerging issues.

By removing the need to purchase and maintain on-premise infrastructure, organisations reduce capital expenditure and lower energy consumption. These systems also offer high scalability, allowing users to add or remove resources as needed, keeping costs under control.

Real-time monitoring and analytics help identify potential issues before they become hazardous. Remote access allows personnel to monitor and adjust systems from a safe distance in potentially volatile environments, which enhances workplace safety. Automating routine tasks frees up personnel to focus on more complex issues, and real-time insights support quick, informed decision-making to drive greater efficiency.

High Tide Technologies (n.d.) emphasise the importance of ensuring proper planning and security measures. When implemented properly, cloud-based SCADA systems are a powerful, cost-effective solution for organisations looking to harness the full potential of IoT.

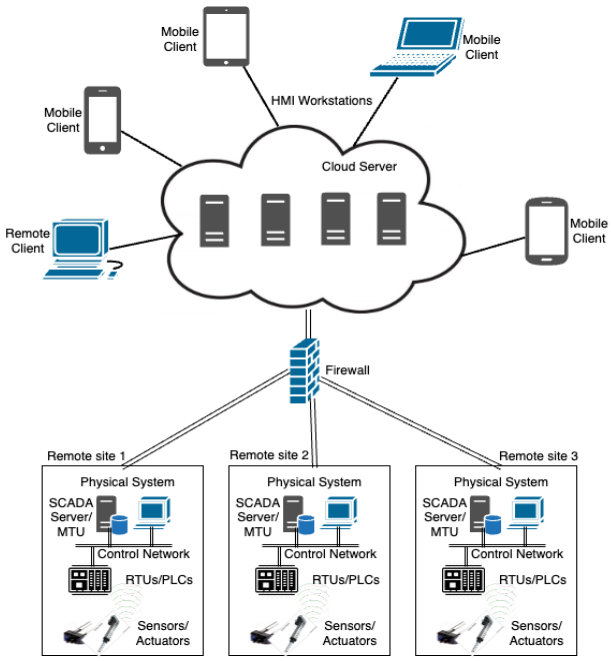


Figure 9: Architecture of a Cloud-based SCADA system (Wali & Alshehry, 2024)

05

A Edge Computing & Digital Twins

Edge Computing & Digital Twins

Edge computing is a distributed computing framework that brings enterprise applications closer to data sources such as IoT devices or local edge servers, enabling the processing and analysis of data closer to the source. In the power grid, it can be deployed at various locations, including substations, to process and analyse data from IoT sensors in real-time. Edge computing increases grid optimisation, enhances resilience and reduces energy waste.

Rick Kephart, Vice President of Technology at Emerson Power and Water Solutions, notes that the power distribution system has traditionally operated as a passive network. However, over the last five to ten years, rapid changes in power distribution operations have created a demand for new and varied solutions – this demand increases both grid complexity and costs.

With the use of edge computing comes the potential for a more granular view of the grid. Data from substations can be condensed and sent to control centres and lead to increased visibility and control, as well as reduced latency.

With edge controllers positioned closer to field installations, teams can run high-resolution analytics on equipment locally. Rather than streaming high-resolution data to control centres, machine learning models can be executed at the source, making decisions and aggregating data on-site. This enables faster control strategies in response to short-term events, while simultaneously reducing the required communications bandwidth and its associated cost (Kephart, 2024).

Digital Twins

A digital twin is a virtual representation of an object or system designed to accurately mirror its physical counterpart. In the context of grid operations, a digital twin correlates data from various sources to provide a comprehensive view of power flows and grid behaviour. Digital twins can be used for real-time simulation, predictive maintenance, and the optimisation of MV and LV networks.

Simulating real-time load conditions helps prevent voltage fluctuations, overloads, and blackouts. Utilities can use digital twins to simulate outage scenarios, relay coordination, and fault propagation in order to improve protection schemes. These models can also predict future load demands, supporting optimised network expansion planning and transformer sizing.

Digital twins use machine learning and AI algorithms to process sensor data from transformers, switchgear, cables, and substations. By analysing historical and real-time performance metrics, they detect early signs of equipment degradation. Digital twins can also adapt in real-time to maintain voltage levels and identify power loss and suggest energy-loss preventative actions.

Additionally, digital twins are able to simulate potential cyberthreats and suggest mitigation strategies and bolster grid resilience against cyberattacks. Their ability to boost efficiency, reliability, and resilience makes digital twins an essential and cost-effective solution for modern smart grids.

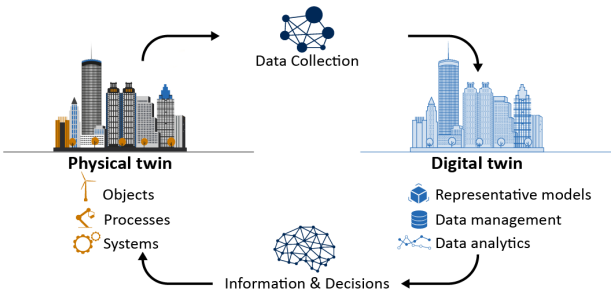


Figure 10: Digital Twin Diagram (GAO, 2023)

Cybersecurity Considerations

As discussed, integrating IoT into SCADA systems introduces cybersecurity risks due to the increased number of connected devices. A co-ordinated attack could manipulate energy flows, cause failures, disrupt power to critical infrastructure, and damage the grid infrastructure (ASIS International, 2024). This underscores the need for robust security measures to ensure the safety and stability of the power grid.

IoT security, a subfield of cybersecurity, focuses on protecting, monitoring, and remediating threats associated with connected devices. It is particularly important because any smart device can serve as an entry point for cybercriminals. If cybercriminals gain entry, they could access high-value assets or conduct malicious activity, such as stealing data, IP (Intellectual Property) or other sensitive information.

To help mitigate these risks, utilising encryption, multi-factor authentication, intrusion detection, firewalls and regular firmware updates is vital. Encryption ensures secure communication by protecting data in transit through secure protocols. Multi-factor authentication utilises at least two different pieces of evidence to verify the users identify, this could be their account password, as well as an OTP (One Time Pin) sent to their mobile phone.

Firewalls are network security devices that monitor, and filter incoming and outgoing network traffic based on an organisation's previously established security policies, utilising them alongside IDS protects the network from any unauthorised access. Running regular updates ensures that all IoT devices and SCADA systems have the latest security patches to avoid any potential vulnerabilities being exploited.

It is also important to ensure employees are trained and aware of cybersecurity threats. Ayano (2024), a certified Information System Security Specialist, states that humans are the "missing link" in the cybersecurity chain, as they are often highly susceptible to social engineering, phishing, insider threats and prone to commit errors - the importance of proper training cannot be overemphasized.

A multidimensional approach that combines technical security solutions with continuous staff education is the most effective way to secure both MV and LV networks. By protecting communication layers, reinforcing critical MV infrastructure, and reducing human error, utilities can significantly improve their resilience against cyber threats.

06

Advantages of IoT and OMS over Traditional SCADA

Traditional SCADA systems have long played a critical role in monitoring and controlling power distribution networks. However, as grid complexity increases and operational demands evolve, the limitations of conventional SCADA, particularly in terms of cost, scalability, and adaptability, have become more apparent.

In contrast, IoT and Outage Management System (OMS) technologies offer a modern, decentralised alternative that addresses many of these challenges. By leveraging low-cost sensors, cloud connectivity, and intelligent automation, utilities can expand coverage across both MV and LV networks without the expense or rigidity associated with legacy infrastructure.

From improving fault detection and restoration times using IoT-enabled Fault Circuit Indicators (FCIs) and smart breakers, to enabling dynamic load balancing and remote grid reconfiguration, these technologies provide a more flexible, scalable, and cost-effective approach to modern distribution network management.

Cost efficiency

IoT and OMS significantly reduce costs compared to traditional SCADA for both MV and LV networks, with lower hardware and infrastructure costs. IoT devices (e.g. sensors, smart meters, and actuators) are typically low-cost, mass-produced components that can be deployed incrementally across the network. OMS platforms often integrate with existing systems, avoiding the need for full replacement.

IoT devices are also generally easier to install and configure, which reduces labour costs.

SCADA systems often require costly on-premise servers, licensing fees, and system-specific maintenance. Alternatively, cloud-based OMS and IoT platforms offer scalable, pay-as-you-go models, allowing affordable scalability based on needs and budgets.

Additionally, IoT systems often support remote diagnostics, predictive maintenance, and automated alerts, reducing the need for routine manual inspections. This helps avoid unexpected outages, extends asset lifespans, and minimises costly emergency response callouts.

Scalability

Traditional SCADA systems are costly and complex to scale beyond high-voltage infrastructure, making full coverage of MV, and especially LV, networks impractical. In contrast, IoT and OMS platforms offer modular, cost-effective scalability for both.

Wireless communication technologies such as LPWAN, cellular, and mesh networks enable rapid deployment without extensive infrastructure, while cloud-based OMS solutions can dynamically scale to accommodate growing device networks and data volumes.

These systems also support seamless integration of distributed energy resources (DERs), making them well suited to the demands of modern, decentralised grids. Unlike traditional SCADA, which often requires hardwired connections, IoT can easily scale across rural or geographically dispersed areas. This is particularly useful for utilities operating in regions with poor infrastructure or growing informal settlements - or for those with plants located in other countries (Rapier Industries, 2023).

Improved Fault Detection and Restoration

IoT-enabled Fault Circuit Indicators (FCIs) and smart breakers offer improvement in fault detection and restoration times compared to traditional SCADA setups. These devices provide real-time visibility into fault locations and conditions, allowing utilities to isolate and address issues faster. Softengi (2020) highlights that this improves both the reliability and availability of assets.

When integrated with OMS, FCIs and smart breakers can automatically trigger reconfiguration or restoration protocols, reducing outage durations and improving reliability indices such as SAIDI and SAIFI. This level of responsiveness is especially valuable in MV networks, where rapid fault localisation and isolation can prevent cascading failures, otherwise known as the failure of a component triggers the successive failures of other parts of the network, as defined by Schäfer. et al. (2018), and minimise customer disruption.

Enhanced Flexibility and Resilience

IoT and OMS technologies provide a decentralised alternative to traditional SCADA systems, significantly enhancing grid flexibility and resilience. Unlike rigid, centralised architectures, IoT-based systems can operate autonomously at the edge, enabling localised decision-making, rapid responses and continued functionality even if central communication is lost. This decentralised structure reduces single points of failure and supports self-healing capabilities, such as automated fault isolation and rerouting. OMS platforms integrated with IoT also offer greater adaptability in responding to shifting load patterns, integrating DERs, and managing weather-related disruptions - making the grid more robust in both day-to-day operations and during major disturbances.

Real-Time Monitoring and Actionable Insights

IoT-enabled systems deliver continuous, real-time monitoring across MV and LV networks, providing utilities with immediate visibility into asset performance, load conditions and potential faults. Unlike traditional SCADA systems, which often rely on limited telemetry, IoT sensors stream data continuously, enabling proactive network management. This data, when processed through cloud-based OMS platforms and edge analytics, becomes actionable. Utilities can detect anomalies, predict equipment failures, and respond to emerging issues in real time. This leads to faster, more informed decision-making, optimised maintenance strategies, and improved operational efficiency across the distribution grid (Rapier Industries, 2023).

Together, IoT and OMS technologies offer a shift in how utilities monitor, manage, and optimise power distribution networks. By addressing the limitations of traditional SCADA, they empower utilities to extend intelligent control across both MV and LV networks. Leveraging modern technologies to deliver the flexibility, resilience, and visibility needed for effective smart grid management.

07

The Future of MV and LV Network Monitoring and Control

The Future of MV and LV Network Monitoring and Control

In a 2022 article, Future Market Insights Inc. predicted that over the next decade, the demand for IoT in utilities would experience a "substantial boom," driven by continued emphasis on efficiency, sustainability and the global push to modernise grid infrastructure. The global IoT in utilities market was estimated at USD 38.4 billion in 2024 and is projected to more than double to USD 77.6 billion by 2034. This growth reflects the rising adoption of smart grid technologies, the increasing need for energy efficiency, and the broader shift toward decentralised and responsive energy systems. As smart grid initiatives mature, the demand for IoT adoption across both medium voltage (MV) and low voltage (LV) networks is expected to accelerate.

Emerging trends such as AI-driven automation for fault detection and load balancing, as well as

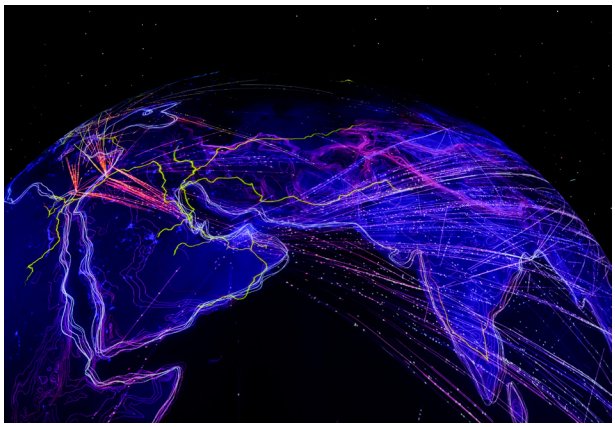


Figure 11: Futuristic Grid Image

the adoption of digital twins and edge computing for predictive maintenance and operational optimisation, are already reshaping the utility landscape. Future Market Insights further predicts that the rise of packaged IoT solutions will fuel rapid adoption in the sector, leading to global expansion and heightened competitiveness. This, in turn, is expected to drive innovation in advanced, interoperable IoT offerings that align with increasingly complex regulatory and environmental goals.

MV networks will benefit from enhanced switching capabilities, real-time grid analytics, and intelligent load management tools. LV networks, on the other hand, stand to gain from improved voltage regulation, decentralised asset monitoring, and greater visibility at the consumer level, particularly through furthering the rollout of smart meters. These devices enable real-time consumption tracking, facilitate accurate billing, and support demand response programmes, helping both utilities and consumers manage energy use more efficiently and reduce carbon emissions (Wang, 2025). As distributed energy resources (DERs) such as rooftop solar, home batteries, and EVs become more common, especially within LV networks, monitoring systems will need to adapt to bidirectional power flows and dynamic load profiles.

Increasing grid digitalisation also brings heightened risks (Mazhar et al., 2023); robust cybersecurity frameworks and encrypted communication protocols will be essential to safeguarding operational resilience and data integrity.

Beyond technical performance, long-term interoperability and standardisation will be necessary to ensure that IoT devices, platforms, and communication protocols work cohesively across manufacturers and regions. To realise this digital transformation, utilities must also invest in workforce development, equipping teams with the skills needed to deploy, and manage, monitoring and control systems.



Figure 12: Woman Analysing Data

Additionally, IoT-enabled sensors across MV and LV infrastructure can support environmental monitoring, feeding into ESG reporting by tracking energy losses, emissions, and even air quality metrics. These systems will also contribute to disaster preparedness - enabling rapid fault isolation, localised control through microgrids, and faster service restoration.

Despite some barriers, the case for adopting scalable, future-ready IoT and Outage Management System (OMS) solutions is stronger than ever. These technologies not only improve operational efficiency and service reliability but also lay the groundwork for more resilient, adaptive, and sustainable grid ecosystems. With the integration of renewable energy sources and the emergence of distributed energy resources (DERs), intelligent grid management is essential. As pressure mounts to modernise ageing infrastructure and meet rising energy demands, utilities that invest early in intelligent network solutions, supported by real-time analytics, predictive maintenance, and smart metering, will be best positioned to lead the next era of power distribution.

Conclusion

This paper has explored how IoT devices and Outage Management Systems (OMS) can function as a practical and cost-effective alternative to traditional Supervisory Control and Data Acquisition (SCADA) systems, particularly within medium voltage (MV) and low voltage (LV) electricity distribution networks. While SCADA systems have historically served as the backbone of grid management at the transmission level, their high cost, inflexible architecture, and centralised design make them poorly suited for widespread deployment across more distributed and dynamic MV and LV networks.

IoT and OMS technologies provide utilities with a decentralised, modular approach to grid monitoring and control, supporting real-time data acquisition, automated fault detection, and flexible operational decision-making. These technologies are not only more affordable but are also more aligned with the evolving requirements of modern distribution networks.

Unlike legacy SCADA, which relies heavily on centralised data processing and fixed communication pathways, IoT and OMS systems leverage distributed architectures and edge computing to process and act on data in near-real-time. This enables faster localised decision-making, improves outage response times, and reduces dependency on central control centres. Moreover, these systems are inherently scalable and interoperable, allowing utilities to begin with limited deployments, such as smart meters, pole-mounted sensors, or mobile fault-detection units, and expand incrementally as funding, network requirements, or other needs evolve.

Despite the advantages, the deployment of IoT and OMS solutions are not without challenges. Initial implementation costs, particularly for sensor networks, communication infrastructure, and system integration, can be restrictive without proper funding or return-on-investment planning. Additionally, as these technologies increase the number of connected endpoints, they introduce new cybersecurity risks and require robust data governance frameworks to ensure system integrity and operational continuity.

Nonetheless, the potential long-term gains in operational efficiency, service reliability, outage mitigation, regulatory compliance, and customer satisfaction are substantial. IoT and OMS solutions enable granular system visibility, condition-based asset management, automated switching, and even environmental monitoring in ways that traditional SCADA cannot. Their adaptability and rapid deployment capabilities also position them as ideal solutions for utilities seeking to modernise ageing infrastructure without undergoing complete replacements of legacy systems.

As energy systems worldwide continue to decentralise and digitalise, the limitations of centralised control systems becomes increasingly apparent. The shift toward smart, data-driven utilities is already underway, and the ability to monitor and control distribution networks in real time will be essential to supporting a flexible, low-carbon energy future. Utilities that fail to adapt risk not only higher long-term operating costs and service interruptions but also risk falling behind as policy mandates and public expectations evolve.

IoT and OMS technologies may have emerged as a workaround to SCADA's high cost, but they are rapidly becoming the backbone of next-generation grid intelligence. By embracing these systems now, utilities can build toward a more resilient, adaptable, and customer-centric energy network - one that is capable of meeting both current operational demands and the unforeseen challenges of tomorrow.

Bibliography

Aghenta, L & I, M. Tariq. (2019). Development of an IoT Based Open-Source SCADA System for PV System Monitoring. pp. 1-4. Available at: https://www.researchgate.net/publication/336439913_Development_of_an_IoT_Based_Open_Source_SCADA_System_for_PV_System_Monitoring [Accessed: 17/03/2025]

Ayano, K. (2024) Cybersecurity In Critical Infrastructure: Protecting Power Grids and Smart Grids. Available at: https://www.cyberdefensemagazine.com/cybersecurity-in-critical-infrastructure-protecting-power-grids-and-smart-grids/ [Accessed: 19/03/2025]

Behera, Anwesh D. (2024). IoT-Driven Digital Transformation in Low Voltage Distribution Networks. Available at: https://www.researchgate.net/publication/385188456_IoT-Driven_Digital_Transformation_in_Low_Voltage_Distribution_Networks [Accessed: 20/05/2025]

CLAROTY (2024) A Comprehensive Guide to SCADA Cybersecurity. Available at: https://claroty.com/blog/a-comprehensive-guide-to-scada-cybersecurity#:~:text=Legacy%20Systems%3A%20SCADA%20systems%20were,them%20vulnerable%20to%20cyber%20attacks [Accessed 10/03/2025]

CORSO SYSTEMS. (No date). SCADA in the Cloud. Available at: https://corsosystems.com/posts/scada-in-the-cloud [Accessed 25/04/2025]

Elliott, W.P. and Gaffen, D.J., 1991. On the utility of radiosonde humidity archives for climate studies. Bulletin of the American Meteorological Society, 72(10), pp.1507-1510.

Eskom. (No date). Containerised Microgrids. Available at: https://www.eskom.co.za/distribution/microgrid/ [Accessed: 19/05/2025]

Future Market Insights Inc. (2022) IoT in Utilities Market Insights – Trends & Forecast 2024 to 2034. Available at: https://www.futuremarketinsights.com/reports/iot-in-utilities-market [Accessed: 22/05/2025]

Heisenware. (2025). IoT vs. SCADA: How Modern Technologies Are Changing the Industry. Available at: https://heisenware.com/en/blog/iot-vs-scada [Accessed: 26/02/2025]
High Tide Technologies. (No date). The Role of Cloud-Based SCADA in Industry 4.0 and IoT. Available at: https://www.htt.io/learning-center/the-role-of-cloud-based-scada-in-industry-4-0-and-iot [Accessed: 17/03/2025]

Hossain, S. Rahman, M. Sarker, T. Haque, E. & Jahid, A. (2019). A smart IoT based system for monitoring and controlling the sub-station equipment. Available at: https://www.sciencedirect.com/science/article/abs/pii/S2542660518301628 [Accessed: 06/03/2025]
IBM. (No date). What is AMI? Available at: https://www.ibm.com/think/topics/advanced-metering-infrastructure [Accessed: 06/03/2025]

IEA (2024), SDG7: Data and Projections: Access to electricity. Available at: https://www.iea.org/reports/sdg7-data-and-projections [Accessed: 20/05/2025]
Inductive Automation. (2020) PLC Basics, Operation, Programming and the Future of PLCs. Available at: https://inductiveautomation.com/resources/article/what-is-a-PLC#:~:text=Programmable%20Logic%20Controllers%20(PLCs)%20are,different%20sizes%20and%20form%20factors [Accessed: 10/03/2025]

Kappagantu, Ramakrishna. Senn, Subir. Mahesh, M. Daniel, A. S. (2015). Smart grid implementation in India – A case study of Puducherry pilot project. International Journal of Engineering, Science and Technology Vol. 7, No. 3. [Accessed: 19/05/2025]

Kephart, R. 2024. Edge Computing May Be the Future of Power Distribution. Available at: https://www.powermag.com/edge-computing-may-be-the-future-of-power-distribution/ [Accessed: 18/03/2025]

Mazhar, T. Talpur, DB. Shloul, TA. Ghadi, YY. Haq, I. Ullah, I. Ouahada, K. Hamam, H. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence. Brain Sci. 2023. doi: 10.3390/brainsci13040683. Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC10136937/ [Accessed: 27/05/2025]

Network Waitaki. (2018). The Benefits of a Distribution Transformer Monitoring Solution at Network Waitaki Limited. Available at: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://id.itron.com/o/commerce-media/accounts/-1/attachments/3808342 [Accessed 06/03/2025]

Bibliography

Rahardjo, A. (2021) Analysis of Blackouts Based on The Medium Voltage Distribution Network's Disruptions Time in UP3 Menteng Central of Jakarta. Indonesia: Purpose-led Publishing.

Rapier Industries. (2023). Revolutionizing Industrial Manufacturing: IoT & Low Voltage. Available at: https://www.rapierindustries.com/news/revolutionizing-industrial-manufacturing-iot-low-voltage/#:~:text=With%20IoT%2Denabled%20sensors%20embedded,%2C%20vibration%2C%20and%20energy%20consumption [Accessed: 14/05/2025]

Rugged Telemetry. (2024). What is IoT (For Energy Management Systems). Available at: https://www.ruggedtelemetry.com/blog-posts/benifits-of-energy-management-using-iot [Accessed: 07/03/2025]

Schneider Electric. (No date). What is switchgear? Available at: https://www.se.com/us/en/work/featured-articles/what-is-switchgear/#:~:text=Switchgear%20contains%20fuses%2C%20switches%2C%20and,limiting%20damage%20to%20the%20system [Accessed: 05/03/205]

Schäfer, B., Witthaut, D., Timme, M. et al. Dynamically induced cascading failures in power grids. Nat Commun 9, 1975 (2018). https://doi.org/10.1038/s41467-018-04287-5
Smart Energy International. (2016). Smart grid development in Spain. Available at: https://www.smart-energy.com/magazine-article/smart-grid-development-spain/ [Accessed: 16/05/2025]

Softengi (2020). IoT Solutions for Electric Power Industry. Available at: https://softengi.com/blog/iot-solutions-for-the-electric-power-industry/#:~:text=IoT%20technology%20will%20help%20to,production%20has%20increased%20to%208.4%25 [Accessed:
15/05/2025]

Swain, A., Abdellatif, E., Mousa, A., & Pong, P. W. T. (2022). Sensor Technologies for Transmission and Distribution Systems: A Review of the Latest Developments. Energies, 15(19), 7339.

Tameson. (2023). What Is An Actuator - Types and Applications. Available at: https://tameson.com/pages/actuator#_edt8gixhplut [Accessed: 06/03/2025]

TechTarget. (No date). Gateway. Available at: https://www.techtarget.com/iotagenda/definition/gateway [Accessed: 06/03/2025]

Thakker, A. (2024). IoT Fundamentals: Sensors, Actuators, and Smart Networks. Available at: https://medium.com/@aasthathakker/iot-fundamentals-sensors-actuators-and-smart-networks-2c2f0f4f2154#:~:text=Actuators%3A%20Brining%20IoT%20to%20life,used%20by%20computers%20or%20-humans [Accessed 05/03/2025]

Tuballa, Maria Lorena & Abundo, Michael Lochinvar. (2016). A review of the development of Smart Grid technologies. Renewable and Sustainable Energy Reviews, Volume 59, Pages 710-725. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1364032116000393#preview-section-references [Accessed: 16/05/2025]

Velos. (2024). A Brief Guide to Low Power Wide Area Network (LPWAN). Available at: https://info.velosiot.com/a-brief-guide-to-low-power-wide-area-network [Accessed: 13/03/2025]

Wang, Q. Li, Y. Li, R. (2025). Integrating artificial intelligence in energy transition: A comprehensive review. Science Direct: Energy Strategy Reviews, Volume 57. Available at: https://www.sciencedirect.com/science/article/pii/S2211467X24003092#bib6 [Accessed: 27/05/2025]

World Economic Forum. (2022). What are microgrids – and how can they help with power cuts? Available at: https://www.weforum.org/stories/2022/05/what-are-microgrids-renewable-power/#:~:text=There%20are%20around%204%2C500%20microgrid,for%20Climate%20and%20Energy%20Solutions [Accessed: 19/05/2025]

Zenarmor. (2022). A Guide to Mesh Topology: Definition, Practices, and Importance. Available at: https://www.zenarmor.com/docs/network-basics/what-is-mesh-topology [Accessed: 13/03/2025]
15/05/2025]

Figure Bibliography

Derhab, A., Benmalek, M., Challal, Y. & Bouabdallah, A. (2018). Basic components of an AMI system [Diagram]. Available at: https://www.researchgate.net/figure/Basic-Components-of-an-AMI-System_fig6_322459589 [Accessed 19 August 2025]. (Figure 7)

Deramsey in Allumiax. (2024). Diagram of a general SCADA system layout [Diagram]. Available at: https://www.allumiax.com/blog/scada-and-its-application-in-electrical-power-systems [Accessed 19 August 2025]. (Figure 3)

Diniz, P., Tcheou, M., Lovisolo, L., Ribeiro, M., da Silva, E., Rodrigues, M. & Romano, J. (2014). A typical power system scheme [Diagram]. Available at: https://www.researchgate.net/profile/Paulo-Diniz-4/publication/259621133/figure/fig1/AS:614018330943537@1523404786877/A-typical-power-system-scheme-LV-low-voltage-MV-medium-voltage-and-HV-high-voltage.png [Accessed 19 August 2025]. (Figure 1)

GAO. (2023). Digital twin diagram [Diagram]. Available at: https://www.gao.gov/products/gao-23-106453 [Accessed 19 August 2025]. (Figure 10)

Miguel Power Association. (2023). Example microgrid diagram [Diagram]. Available at: https://smpa.com/microgrids-community-resilience-and-climate-action [Accessed 19 August 2025]. (Figure 5)

Maddox. (2024). Voltage step up & step down transformers [Diagram]. Available at: https://www.maddox.com/resources/articles/low-voltage-distribution-systems [Accessed 19 August 2025]. (Figure 2)

N-iX. (2023). Conventional grid vs. a smart grid [Diagram]. Available at: https://www.n-ix.com/digital-transformation-energy-industry/ [Accessed 19 August 2025]. (Figure 4)

CS Odessa. (n.d.). Smart grid diagram. ConceptDraw Solution Park – Internet of Things Solution [Diagram]. Available at: https://www.conceptdraw.com/solution-park/computer-networks-internet-things [Accessed 19 August 2025]. (Figure 6)

Tech Target. (2021). Full vs. partial mesh networks [Diagram]. Available at: https://www.techtarget.com/iotagenda/definition/mesh-network-topology-mesh-network [Accessed 19 August 2025]. (Figure 8)

Wali, A.M. & Alshehry, F. (2024). Architecture of cloud-based SCADA systems [Diagram]. Available at: https://www.researchgate.net/figure/Architecture-of-cloud-based-SCADA-systems-inspired-by-15_fig2_379772155 [Accessed 19 August 2025]. (Figure 9)