14

Internet of Things-Based Monitoring in Electrical Power Systems

Vishal Mittal
General Manager (Tendering) - Power Systems,
Schneider Electric Infrastructure Limited, Gurgaon
mittalvishal22@gmail.com

Aditi Gupta
Assistant Professor,
EEE, UIET,
Panjab University, Chandigarh, India
aditigupta@pu.ac.in

Abstract

The rapid growth of IoT technologies enables advances in electrical power systems. The monitoring of electrical power systems in real-time will be scalable. Furthermore, sensing and IoT technologies will help address growing issues of grid instability, the growth of renewable generation, and ageing infrastructure. This chapter on the Internet of Things looks at the finer details of IoT architecture. It covers aspects ranging from sensors and wireless networks to edge computing and machine-learning analytics. Finally, we apply all of these to fault detection, predictive maintenance, and energy optimisation in smart grids. It discusses viable use cases, precautions against cyber threats, and new developments, such as AI-powered digital twins, that will make processes more reliable and sustainable.

Keywords: *Internet of Things, power system monitoring, smart grids, wireless sensor networks, IoT sensors, real-time analytics, fault detection, predictive maintenance, energy management, cyber security, edge computing.*

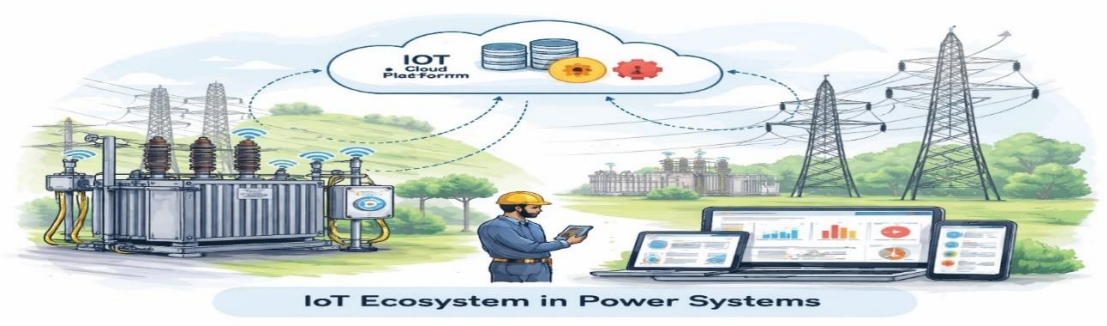
1. Introduction

Electrical power systems combine power generation and distribution techniques to deliver generated power. In other words, they deliver instant power to homes and offices. Thus, the electrical system is the part of a power system that uses

electricity. Power systems are increasingly under pressure from the ageing of their assets, which makes it more likely that their performance will be interrupted, the connection of variable renewable energy sources (i.e., solar and wind), and the need for reduced fault detection time. Existing centralised monitoring, based on inspections done now and then, cannot cope with different demands such as voltage sags, overloads, equipment failures, and so on, leading to delays in responding to these issues. With the advent of IoT (Internet of Things), the pain points related to data collection, analysis, and assimilation across the grid have been addressed.

IoT changes the monitoring of power systems from a human, reactive process to a more proactive, real-time one. With networks of connected sensors and devices, IoT can provide a detailed view of system parameters such as voltage, current, power factor, and temperature. Not only does this real-time shift detect anomalies, but it also predicts failures, helping reduce maintenance costs and improve the overall efficiency of the grid. In areas where renewables are heavily used, the IoT can offset supply fluctuations by optimising load in real time.

The present chapter aims to study the IoT-based monitoring framework for the electrical power system. This study aims to examine the sensor, communication network, and the analysis of key parameters: voltage stability, current, fault localisation, and energy efficiency. Our objective is to create a practical guide for engineers and policymakers by synthesising current implementations and future potential. The development of IoT has paved the way for predictive scaling and monitoring, enhancing the reliability and sustainability of power systems.



The figure above illustrates a typical IoT ecosystem in power systems, showing sensors on transformers and lines feeding data to a cloud platform for real-time analytics and alerts.

2. Fundamentals of IoT in Power Systems

IoT in power systems is layered, enabling information flow from physical assets to decision-makers. The perception layer consists of sensors placed on grid components that capture raw environmental and electrical data. The network layer enables secure data transmission through a variety of protocols, while the application layer uses data processed in the cloud or at the edge to generate actionable insights. This tri-layered model stands in marked contrast to legacy systems, which offer greater modularity and extensibility for evolving electricity grid needs.

The main components of IoT are crucial for power monitoring. Current transformers (CTs) measure AC currents non-invasively. Resistor- or capacitive-divider-type voltage sensors measure the potential difference. Thermocouples or RTDs measure the temperature of hotspots in transformers and cables to prevent thermal failures. Automated circuit breakers act as actuators, responding to IoT signals to isolate equipment from the network. Gateways aggregate data from various sensors, manage protocol conversion, perform first-stage filtering, and send it to central servers. In remote locations, these components are powered by low-energy microcontrollers such as ESP32 or ARM-based chips.

A critical comparison shows IoT is superior to conventional Supervisory Control and Data Acquisition (SCADA). SCADA depends on wired RTUs (Remote Terminal Units) and a polling-based communication model that limits scalability to hundreds of points and incurs high installation costs (e.g., $10,000+/substation). IoT, on the other hand, uses wireless mesh networks to connect thousands of nodes at a fraction of the cost, with sensors under $50 each and sub-second real-time updates via protocols like MQTT. While SCADA is effective for deterministic control of critical infrastructure, it falls short in a big data environment. The IoT includes a machine learning component for predictive analytics. Field tests have shown that this reduces false alarm rates of about 30-50%. IoT enables battery life and security challenges. As a solution, we have enforced LPWAN (low-power wide-area networks) and encryption standards.

Aspect	Traditional SCADA	IoT-Based Monitoring
Scalability	Limited (100-500 nodes)	High (10,000+ nodes)
Cost	High ($5K-20K per site)	Low ($20-100 per sensor)
Real-Time Capability	Polling (seconds-minutes)	Event-driven (milliseconds)
Data Analytics	Basic thresholding	ML/AI predictive models
Deployment	Wired, invasive	Wireless, plug-and-play

This table underscores IoT's transformative edge, particularly for distributed grids.

In reality, the fundamentals of IoT enable voltage-monitoring applications on transmission lines. Specifically, when the sensors detect sags greater than 5%, they send alerts. At present, CTs integrated with Hall-effect sensors allow monitoring of motor phase imbalance, which is essential to prevent motor failure. Vibration sensors on bushings are utilised for fault detection through PD pattern recognition. Energy efficiency analytics can optimise power factor data to visualise, identify and dynamically recommend solutions such as capacitor banks for inductive loads.

3. IoT Sensors and Devices for Power System Monitoring

IoT sensors and devices are the building blocks of power system monitoring. They collect high-fidelity data from hard-to-reach grid assets, including transmission lines, transformers, and substations. These are specifically designed for harsh environments, featuring rugged housing (IP67), a wide temperature range (-40° to 85°), and low power consumption, allowing for long-term deployment without frequent visits. Types of core sensors include electrical parameter monitors such as non-contact current transformers (CTs) for AC measurement

up to 10 kA using Rogowski Coils, voltage sensors on capacitive dividers for 11-33 kV lines, and power factor transducers with shunt capacitors. Environmental sensors track ambient conditions with thermocouples for hotspot detection (critical for oil-immersed transformers exceeding 80°C) and humidity probes using capacitive hygrometers to predict insulation degradation.

Wireless Sensor Networks (WSNs) use mesh topologies for efficient sensing, with nodes transmitting data incrementally, one after the other. This approach incurs wiring costs 70% lower than those of wired alternatives. Protocols such as Zig Bee (IEEE 802.15.4) provide 250 kbps over a range of 10-100 m and are designed for intra-substation applications. In comparison, LoRaWAN is suitable for rural transmission lines and provides coverage up to 27 km at 0.3-50 kbps for sparse deployments. NB-IoT is a cellular LPWAN variant that can achieve 99.9% uptime for an urban grid. The link budget for NB-IoT-capable devices is typically 164 dB. NB-IoT can support a large number of devices, up to 50,000 per km square. Edge devices, such as the Raspberry Pi 4 or Arduino MKR WAN 1310, aggregate data locally and run lightweight firmware to perform preliminary filtering, such as Kalman filters for denoising voltage signals and preprocessing. By doing so, they significantly reduce the volume of data sent to the cloud by up to 80%.

4. Communication Protocols and Network Infrastructure

Effective communication is key to IoT monitoring, which involves low-latency, secure data transmission. In dense environments, short-range protocols prevail. Wi-Fi 6 provides a high-throughput 9.6 Gbps, adequate for a thermal camera's video feed, while Bluetooth Low Energy (BLE 5.0) is suitable for mobile inspections, with a 2 Mbps data rate and a 400-meter range in mesh mode. They're great in substations but fall short beyond 1 km at long range.

Long-range choices fill this space: cellular 4G or 5G offer ubiquitous telecommunications coverage, and 5G slicing for ultra-reliable, low-latency (uRLLC) at 1 ms is critical for fault isolation within microgrids. Alternatives to LPWAN include Sigfox (100 kbps, 10 km urban range) and LoRa, which features top battery life (10+ years) and is designed for small packets (16-byte payload). Systems enable the integration of energy systems, grid management, and smart grid capabilities through multi-protocol gateways that support protocols such as MQTT and CoAP, as well as standards like IEEE 2030.5.

The challenge is that latency spikes due to congestion require quality of service prioritisation. Apart from this, security risks such as man-in-the-middle attacks require AES-256, TLS 1.3 handshakes, and blockchain to ensure tamper-proof ledgering. OpenFMB (Open Field Message Bus) enables interoperability, allowing for plug-and-play across vendors.

Protocol Type	**Range**	**Data Rate**	**Power Use**	**Use Case Example**
Wi-Fi 6	100-300m	Up to 9.6 Gbps	High	Substation CCTV
BLE 5.0	10-400m	2 Mbps	Low	Portable fault scanners
LoRaWAN	2-15 km	0.3-50 kbps	Very Low	Line sag monitoring
NB-IoT/5G	1-10 km	20-200 kbps	Low	Urban smart metering

This table compares protocols, highlighting trade-offs for power system scalability. In practice, MQTT ensures efficient pub-sub for real-time alerts, as in demand-response, where load data triggers capacitor switching within 100 ms.

5. Data Acquisition, Processing, and Analytics

IoT-based power monitoring collects all measurements at a high sampling frequency of 1-10 kHz for voltage/current waveforms for fault and harmonic analysis. Sensors send raw data to edge nodes, which process it using microcontrollers or similar devices, performing analogue-to-digital conversion (typically 12–16-bit resolution) and time stamping for synchronisation. Cloud platforms such as

AWS IoT or Azure Digital Twins consume this data through APIs. They then rely on a stream processing framework, like Apache Kafka, to process 1 TB/day for large grids.

Processing is transitioning from centralised to hybrid edge-cloud models, where edge devices flag anomalies using lightweight algorithms such as ARIMA (Auto-Regressive Integrated Moving Average) for time-series forecasting, generating a latency of 50 ms. The cloud layers then perform big data analytics, with Hadoop or Spark used for storage. Further, the active layer consists of machine learning models such as SVMs and LSTMs, which detect faults/annoyances with 95% accuracy, as seen in IEEE test cases. An example includes detecting partial discharges from vibration data using an isolation forest and classifying thermal images of insulator cracks using CNNs.

Using DGA (dissolved gas analysis)-based transformer health scores, assisted by historical datasets and temperature trend analysis, transformer failures can be predicted 7 to 14 days in advance, helping reduce downtime by 40%. Load forecasting employs the Prophet or XG Boost algorithms on smart meter data, combined with weather API data, to predict inputs from renewable energy sources.

6. Applications in Electrical Power Systems

Using IoT for monitoring helps in electrical power systems, from generation to end-user consumption, through real-world problem-solving applications. Smart grid mechanisms can facilitate demand response by using sensors on distribution transformers to assess load profiles in real time. If the circuits are congested, the relays automatically shut off power to non-essential loads. Thus, helps in reducing peak loads. For example, industrial compressors can shed 20% of their power via Modbus commands. In India, for instance, summers push demand up to 250 GW, straining coal plants. IoT can optimise operations through frequency containment reserves (FCR) operating at our grid frequency of 50 Hz.

Integrating renewable energy is a flagship. 100+ sensors per MW deployed at PV (Photovoltaic) farms, acquiring string-level voltage (600-1000 V DC) and irradiance data. The goal is to enforce MPPT. Monitoring of wind turbine vibrations is performed using nacelle vibration sensors to detect imbalances in rotor blades (RMS >0.5 g). The SCADA data is integrated with Internet of Things (IoT) data to optimise yaw, with an expected increase in annual energy yield (AEY) of 8-12%. The 10 GW of solar parks

in Gujarat use NB-IoT for remote curtailment.

The use of high-speed PMUs (30-60 samples/sec, GPS-PPS-synchronised) for wide-area situational awareness enables detection of symmetrical faults using superimposed-current algorithms. Sensitivity is 0.1 pu. Partial discharge (PD) monitoring of underground XLPE cables using UHF antennas (300 MHz – 1.5 GHz) employs phase-resolved patterns (PRPD) to classify corona versus voids, predicting breakdowns 6 months in advance. Using tension sensors or drones to take infrared thermographic images can assess conductor clearance below 7 m.

Energy management systems require advanced metering infrastructure (AMI): NB-IoT smart meters (according to the DLMS/COSEM protocol) enable enhanced time-of-use (TOU) tariffs, while theft is detected via NTL ratios >15% using harmonic signatures (3rd/5th order). Demand side management (DSM) in microgrids refers to the management of batteries (BMS-integrated) with diesel gensets to facilitate droop control (P-f, Q-V) regulated by CT data, enabling islanding in less than 50 ms.

The microgrids and resilience at the campus scale (e.g., IIT Delhi pilots) that deploy IoT tech for seamless transitions use solar-plus-battery hybrids to maintain 99.99% uptime during the 2025 monsoon. Case studies can be found all over the world. POSOCO of India deployed 15,000 LoRa nodes across the NCR grids to reduce SAIDI from 120 to 45 min/customer/year. ENTSO-E's North Sea Link (1.4 GW HVDC) uses 5G for the offshore wind farm, cutting O&M costs by a quarter. In America, the California Public Utilities Commission mandates that utilities include risk assessments when approving new infrastructure that could also affect disadvantaged communities. PG&E has reduced wildfire ignitions by 60% since installing 50,000 sensors after the 2018 fires.

Application	**Key Metrics**	**IoT Benefit**	**Example Deployment**
Smart Grid	Load balance (±2%)	Peak shaving 15-20%	POSOCO Delhi (15k nodes)

Application	**Key Metrics**	**IoT Benefit**	**Example Deployment**
Renewables	MPPT efficiency >98%	Yield +10%	Gujarat Solar Parks
Fault Detection	Localisation<100 ms	Outages -40%	ENTSO-E PMUs
Energy Management	PF >0.98, NTL <5%	Savings ₹10-20/unit	Indian AMI (100M meters)
Microgrids	Islanding <50 ms	Uptime 99.99%	IIT-Delhi Campus

These applications demonstrate IoT's ROI: payback in 1-2 years via deferred capex.

7. Security, Challenges and Solutions

The increase in Internet of Things (IoT) devices is expected to exacerbate cybersecurity vulnerabilities in power systems. A compromised node can cause cascading failures. An example of this is the 2015 blackout in Ukraine. The incident, which affected 230,000 end users, was caused by the BlackEnergy malware through phishing. Potential threats include Denial-of-Service flooding of MQTT brokers with a 10 Gbps attack, spoofing of synchrophasors to report faults falsely, and worms or ransomware that lock out SCADA dashboards. Resource-constrained IoT devices are arguably the most significant enablers of security shortcomings. With RAM between 8 KB and 32 KB, default credentials enable Mirai-style botnets, while OTA gaps enable zero-day attacks. For instance, 2024 will see buffer-overflow zero-days exploiting LoRaWAN stacks.

There are mitigation frameworks with zero-trust architecture, where every packet is mutually authenticated using TLS 1.3 with ECDSA-256 certs, and

networks are segmented using VLANs (OT/IT isolation). Systems for detecting anomalies (ADS) deploy autoencoders on edge gateways to identify unusual occurrences, such as voltage ramps from 11 kV to 13 kV in 10 ms, with 98% accuracy/low false alarm rate. Blockchain (Hyperledger Sawtooth) ensures that audit trails are immutable by hashing sensor readings into Merkle trees that are verifiable off-chain.

Physical limitations: Power limitations restrict nodes to a standby of 10-50 μW; solutions harvest from CT secondaries (5-20 mW) or RF (P2110-compliant). Scaling for 100k nodes/km²: fog computing hierarchies (edge>regional>cloud). The issue of vendor interoperability silos is bridged by IEC 61850 MMS over MQTT, and OpenFMB provides a DER plug-and-play solution.

Environmental difficulties, such as EMI (150 kHz-30 MHz), require the use of shielded enclosures (e.g., MIL-STD-461F). Data deluge (1 PB/year/grid) necessitates lossy compression (e.g., wavelet-based, 90% reduction).

Challenge	**Root Cause**	**Impact**	**Solution Strategy**	**Efficacy Gain**
Cybersecurity	Weak auth/firmware	Blackouts (hours)	Zero-trust + ADS + Blockchain	99% intrusion block
Power Constraints	Battery drain	20% node loss/year	CT/RF harvesting	Lifespan 10+ years
Interoperability	Protocol silos	Deployment delays	IEC 61850/MQTT gateways	50% integration time cut

Challenge	Root Cause	Impact	Solution Strategy	Efficacy Gain
Scalability	Bandwidth limits	Dropped packets 5-10%	Fog/edge federation	Handles 1M nodes
EMI/Environment	Harsh fields	Sensor noise >10%	Shielding + Kalman filters	Signal purity 99.5%

Regulatory pushes, such as India's CEA (Cyber Security) Guidelines 2025, mandate annual pentests, accelerating adoption.

8. Future Trends and Innovations

IoT monitoring is advancing rapidly and is being further enhanced by AI/ML technologies. A federated learning approach is used to train fault models across utilities without sharing raw data. Edge LSTMs on PiCMs update global weights via Secure Multi-Party Computation, ensuring that users' sensitive information remains confidential and that the process complies with GDPR. SHAP XAI investigates the prediction as presented as extent or probability, for instance, the risk of failure (70%) assessed at the DGA ethane spike by the transformer.

Private networks being prepared for 6G and beyond offer 10 μs latency and 1 Tbps throughput. They provide AI-native slicing, uRLLC for drone swarms to inspect 50 km lines within 10 min, URLLC for haptic tele-op of switchgear. Satellite IoT (Starlink / OneWeb), remote grids blanketed—99.99%-covered LoRa-over-LEO solution in the Himalayas.

The digital twins within NVIDIA Omniverse enable a 1:1 fidelity mirroring of the grid. The Internet of Things (IoT) then feeds data to physics-informed neural networks (PINNs) that simulate specific arcs (such as Parker's law) or ferroresonance. Cyber scenarios are stress-tested offline before being released into a more live setting. Quantum sensors detect microcracks in power lines before electrical discharge occurs.

Factors for sustainability: EV eco-systems integrate 1M EV chargers as a virtual power plant via VPPs. IOA optimised by OCP.Dashboards for carbon tracking calculate Scope 2 emissions using meter data in line with the EU CBAM regulation. Spiking neural networks on neuromorphic chips deliver low power consumption of 1 μJ/inference for edge PD classification.Keys generated through quantum key distribution (QKD) over a fibre of 300 km. Bio-inspired self-healing network. Gartner forecasts that by 2030, 75% of grids will be IoT-native, saving $100B in global losses per year.

9. Conclusions

The introduction of IoT incorporates data analytics, collecting and processing large volumes of data to deliver accurate insights into your electrical power system. By using dense sensor networks, a robust communication protocol, and enhanced AI-driven analytics, IoT offers predictive capabilities that reduce outages by 30-50% and generate internal efficiencies of more than 20%. POSOCO's NCR network and ENTSO-E's offshore are use cases from global pilots.

This broad framework, which includes everything from perceptual layers to digital twins, also directly addresses corrosion risks from ageing industrial infrastructure, voltage and frequency swings due to renewable intermittency, and escalating cyber threats arising from the emergence of 5G/6G. Security systems such as zero-trust architectures and more resilient blockchain-based distributed ledgers, along with more scalable edge federation systems, have matured to deliver enterprise-level resilience with 99.99 per cent uptime, even in hostile environments. The roadmap implementation will be phased in. The first step will include pilot microgrids set up in high-renewable zones, such as the solar hubs in Gujarat.

IEC 61850/MQTT harmonisation. Further regulatory incentives will be prioritised for LPWAN adoption. More broadly, a federation of learning consortia and cross-utility approaches.All in all, IoT strengthens reliability and sustainability in power systems. Moreover, power systems will ultimately achieve net-zero futures. It will also bring annual worldwide savings of 100-150 billion USD. In the future, intelligent grids can be developed through this.

References

1. IEEE Std 2030.5-2018. *IEEE Standard for Wireless Communication Networks for Distributed Energy Resources in Electric Power Systems*.
2. IEC 61850 Ed. 2.1 (2020). *Communication Networks and Systems for Power Utility Automation*.

International Electrotechnical Commission.

3. POSOCO (2022). *Balancing the Grid: Report on Power System Inertia Estimation*. Power System Operation Corporation Ltd., India.
4. ENTSO-E (2025). *Internet of Things (IoT) Applications in Transmission Systems*. European Network of Transmission System Operators for Electricity.
5. Gartner (2024). *Forecast: IoT Market to Reach $991 Billion by 2028*.
6. IEEE Xplore (2024). "Design and Implementation of Digital Power Grid Monitoring and Intelligent Analysis System Based on IoT Platform." DOI: 10.1109/ACCESS.2024.10836034.
7. CEA India (2025). *Cyber Security Guidelines for the Power Sector*. Central Electricity Authority.
8. IEEE C37.118.2-2011. *IEEE Standard for Synchrophasor Data Transfer for Power Systems*.
9. NIST SP 800-213 (2023). *IoT Device Cybersecurity Capability Core Baseline*. National Institute of Standards and Technology.
10. LoRa Alliance (2025). *LPWAN Technical Report for Grid Monitoring*.
11. 3GPP Release 17 (2022). *NB-IoT and 5G Enhancements for Industrial IoT*.
12. IEEE Transactions on Power Systems (2025). "Federated Learning Approaches for IoT-Enabled Fault Prediction in Smart Grids."
13. GRID-INDIA (2026). *Annual Smart Grid Operations Report*. Formerly POSOCO.
14. IEC 30141 (2018). *Internet of Things (IoT) Reference Architecture*.
15. 5G-VICTORI Project (2023). *Trials for Energy Sector IoT over 5G*.
16. Hyperledger Fabric Documentation v2.5 (2025). *Blockchain for Secure IoT Data in Utilities*.
17. AWS IoT Core (2026). *Edge-to-Cloud Pipelines for Power Analytics*.
18. DLMS/COSEM User Association (2024). *Smart Metering Protocols for AMI*.
19. MIL-STD-461F (2015). *Requirements for the Control of Electromagnetic Interference*.
20. NVIDIA (2025). *Omniverse Digital Twins for Power System Simulation*.
21. Intel Loihi 2 (2024). *Neuromorphic Computing for Edge AI in Grids*.

22. Starlink Enterprise IoT (2026). *LEO Satellite Connectivity for Remote Power Assets*.

23. EU CBAM Framework (2026). *Carbon Border Adjustment for Energy Grids*.

24. IEEE Power & Energy Society (2025). *Review: IoT in Renewable Integration*.

25. PG&E (2024). *IoT Wildfire Mitigation Network Evaluation*.

26. Gujarat Renewable Energy Report (2025). *Solar Park IoT Deployments*.

27. IIT Delhi Microgrid Pilot (2025). *IoT for Campus Resilience*.

28. ISO/IEC 20924 (2018). *IoT and Edge Computing Harmonisation*.

29. Apache Kafka Documentation (2025). *Stream Processing for IoT Time-Series*.

30. PSCAD/ETAP User Manuals (2026). *Simulation of IoT-Integrated Grids*.