Study of Energy Management System and IoT integration in Smart Grid

(In context to India)

Gauri Sakaria

Intern, 2nd Batch (2023)

National Centre of Good Governance, New Delhi

Table of Contents

Abstract

This paper focuses on investigating the potential benefits of integrating IoT technology in Smart Grid for energy management. The research will also explore the challenges associated with the integration of IoT technology in Smart Grid, such as security and privacy concerns, interoperability issues, and scalability. The study will propose solutions to these challenges to ensure the successful integration of IoT technology in Smart Grid.

Keywords: Energy Management System, Smart Grids, NSGM, RBAC

Introduction

Energy management systems (EMS) are automated systems that collect energy measurement data from the field and make it available to users via visuals, online monitoring tools, and energy quality analyzers, allowing for the control of energy resources.

A smart grid is an electricity network that monitors and manages the conveyance of power from all generation sources to fulfill the shifting electricity demands of end users. Smart grids coordinate the needs and capabilities of all generators, grid operators, end users, and electricity market stakeholders to ensure that all parts of the system operate as efficiently as possible, minimizing costs and environmental impacts while increasing system reliability, resilience, flexibility, and stability. Because most of the technologies involved are already mature, tracking investments provides information on deployment levels.

IoT integration in Smart Grids

The Internet of Things (IoT) refers to the network of interconnected physical devices, vehicles, buildings, and other objects embedded with sensors, software, and network connectivity. It's what makes the Smart Grid 'Smart' by helping infrastructure evolve from an open loop to a closed loop. By adding data collection capabilities at the edge—which includes smart meters, smart home technologies, EV chargers, solar/wind farms, and more—usage and condition data can be shared across the value chain. Thus, enhancing the efficiency, reliability, and sustainability of the electrical grid.

Here are some key aspects of IoT integration in smart grids:

1. Smart Meters and Sensors: IoT devices, including smart meters and sensors, are deployed across the grid to collect real-time data on energy consumption, voltage levels, and grid performance. Smart meters enable two-way communication between consumers and utilities, allowing for better demand response and load management.
2. Grid Monitoring and Control: IoT-enabled sensors are placed at various points in the grid infrastructure to monitor the health and performance of equipment such as transformers, switches, and substations. This real-time data allows for predictive maintenance, reducing downtime and improving overall grid reliability.
3. Data Analytics and Decision Support: IoT generates vast amounts of data, and analytics tools are employed to extract meaningful insights. Utilities can use this data for predictive analytics, identifying potential issues before they escalate and making informed decisions to optimize grid operations.
4. Demand Response and Load Management: IoT devices enable better demand response programs by allowing utilities to communicate with end-users in real-

time. Consumers can adjust their energy consumption based on pricing signals or grid conditions, leading to a more balanced and efficient use of resources.

5. Distributed Energy Resources (DER) Integration: IoT facilitates the integration of renewable energy sources, energy storage systems, and electric vehicles into the grid. This integration allows for the seamless management of decentralized energy resources, optimizing their use and contributing to grid stability.
6. Cybersecurity: As the grid becomes more connected through IoT devices, ensuring the cybersecurity of these devices and the data they generate becomes crucial. Robust cybersecurity measures are necessary to protect against potential threats and attacks on the smart grid infrastructure.
7. Communication Networks: IoT relies on communication networks to transmit data between devices and systems. The deployment of reliable and secure communication networks, such as advanced metering infrastructure (AMI) and wireless technologies, is essential for efficient IoT integration in smart grids.
8. Scalability and Interoperability: The smart grid ecosystem involves a diverse set of devices and technologies. Ensuring the scalability and interoperability of IoT solutions is crucial to accommodate future expansion and integrate new technologies seamlessly.
9. Regulatory Considerations: The integration of IoT in smart grids often requires supportive regulatory frameworks that encourage innovation, data sharing, and

collaboration among stakeholders. Clear guidelines on data privacy and security are also important.

Primary Drivers for Smart Grids

- Reduced T&D losses and increased efficiency
- Energy access for the masses
- Renewable grid integration
- Peak load management
- System improvements
- Reduced outages/power outages,
- Improved reliability and quality of supply
- Electric vehicle infrastructure

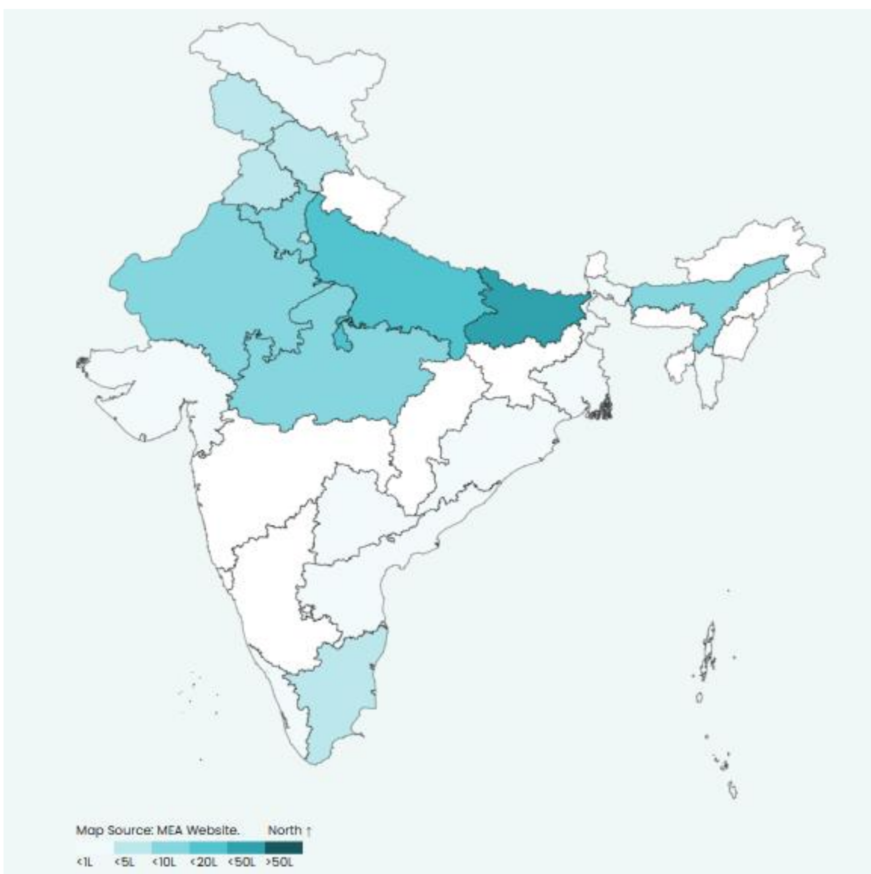
Established Smart Grids in India

Presently India has been continuously working in deploying smart grids all over the country in three phases through the National Smart Grid Mission launched in 2015.

Following are the completed Smart Grid pilot projects sanctioned by the Ministry of Power (MoP):

- Ajmer APDC
- Assam AVVNL
- CESC

- Mysore HPSEB
- Himachal Pradesh PED
- Puducherry TSECL
- Tripura TSSPDCL
- Telangana UHBVN
- Haryana UGVCL
- Gujarat WBSEDCL
- Manesar IIT
- Kanpur SGKC



Regions of Completed National Smart Grid Mission

Considerations while transitioning to IoT-based Smart Grids

Authentication is a critical aspect of smart grids to ensure the security and integrity of the system. Smart grids involve the use of various interconnected devices and systems, and proper authentication mechanisms are essential to prevent unauthorized access (confidentiality) and potential cyber threats. Authorization and Control Users by Role-based Access Control (RBAC) help ensure that only authorized individuals and systems have access to sensitive information and can control IoT devices within the smart grid. Network Segmentation can also help contain potential breaches and limit the impact of unauthorized access to specific areas of the network.

Apart from authentication, it is also important to ensure that the data collected, transmitted, and stored within the grid is accurate, consistent, and secure. Maintaining data integrity is essential for making informed decisions, ensuring reliable grid operations, and preventing potential cybersecurity threats.

Conclusion

For a country like India, where rapid urbanization and population growth pose challenges to the power infrastructure, the deployment and adoption of cutting-edge technology and the introduction of more intelligence into the grid in the form of a Smart Grid, are imperative.

Implementing IoT-based smart grids can contribute significantly to achieving energy efficiency, sustainability, and resilience in the face of evolving demands and challenges. It's essential to integrate these technologies in alignment with national energy policies and regulatory frameworks.

References

- Bali, A. (2018, April). Smart Grid Developments in India. Workshop on Smart Grid Technologies and Implications for Inclusive Development in Sri Lanka, Galle, Sri Lanka.
- Karuri, P. (2016). SMART GRID: A feasible solution to India's energy security [Unpublished dissertation]. UNIVERSITY OF PETROLEUM & ENERGY STUDIES, DEHRADUN.
- "Smart Grid Vision for India", Ministry of Power (MoP), Govt. of India, August 2013
- "Recommendations from Paper on Energy Transition", Ministry of Power (MoP), Govt. of India, January 2020