Journal of Posthumanism

2025
Volume: 5, No: 5, pp. 4327–4342
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i5.1907

MIS Frameworks for Monitoring and Enhancing U.S. Energy Infrastructure Resilience

Clinton Ronjon Barikdar[1], Kazi Bushra Siddiqa[2], Md Alamgir Miah[3], Sharmin Sultana[4], Urmi Haldar[5], Habiba Rahman[6], Md Nazibullah Khan[7], Jahid Hassan[8]

Abstract

This research examines how MIS frameworks strengthen energy infrastructure resilience through consolidated use of predictive models alongside data analytics and crisis management resources. There are multi factors, such as escalating natural disasters and elevated cyber threats with aging infrastructure systems, constantly push. The U.S. energy system toward declining resilience levels. The strategic decision-making and performance enhancement now depends heavily on Management Information Systems. This study uses qualitative research methods and relies on secondary data from energy reports alongside energy grid failure analysis and MIS implementation studies. This analysis reviews various MIS systems, such as SCADA and ERP, to identify how they could improve monitoring operations and evaluation procedures and quick response functionality. MIS development based on specific system needs leads to greater energy system surveillance capabilities and better resource management with improved recovery protocols. The research demonstrates how energy infrastructure protection improves when intelligent MIS combines real-time analysis along with predictive artificial intelligence technologies towards reaching national security goals for U.S. energy systems.

Keywords: *Management Information Systems, Energy Infrastructure, Infrastructure Resilience, Energy Security, U.S. Energy Policy, Cybersecurity.*

Introduction

The United States' energy network, which includes power grids with pipelines and fuel delivery systems. It addresses growing threats against its foundation from natural catastrophes as well as cyberattacks and aging system deterioration (Berkeley et al., 2010). The ability to anticipate disruptions along with the ability to absorb and adapt and quickly return to normal operations constitutes national priority resilience (Force, 2020). Resilience goes beyond reliability by

[1] School of Business, International American University, Los Angeles, CA 90010, USA, Email: barikdarclinton@gmail.com, (Corresponding Author), ORCID ID: https://orcid.org/0009-0002-6291-2446.
[2] School of Business, International American University, Los Angeles, CA 90010, USA, Email: bushrasiddiqa82@gmail.com, ORCID ID: https://orcid.org/0009-0008-0283-9850
[3] School of Business, International American University, Los Angeles, CA 90010, USA, Email: mdalamgirmiahiau@gmail.com, ORCHID ID: https://orcid.org/0009-0005-5780-125X.
[4] School of Business, International American University, Los Angeles, CA 90010, USA, Email: sharminanis369@gmail.com, ORCHID ID: https://orcid.org/0009-0005-7213-4504.
[5] Department of Management, Glasgow Caledonian University, London, UK, Email address: UHALDA300@caledonian.ac.uk, ORCID ID https://orcid.org/0009-0000-4040-7583.
[6] School of Business, International American University, Los Angeles, CA 90010, USA, Email: habiba.rahman1993@gmail.com, ORCID ID: https://orcid.org/0009-0009-8101-479X.
[7] School of Business, International American University, Los Angeles, CA 90010, USA, Email: khanroyal2014@gmail.com, ORCID ID: https://orcid.org/0009-0008-4132-1413
[8] School of Business, International American University, Los Angeles, CA 90010, USA, Email: engineer.jhassan@gmail.com, ORCID ID: https://orcid.org/0009-0005-0215-3179

concentrating on system adaptation with backup capabilities combined with swift crisis recovery procedures (Mohanty et al., 2024). Development of Management Information Systems serves as the key instrument for achieving resilience through integration of IoT sensors with SCADA systems and GIS tools and artificial intelligence analytics.

The integrated system tools monitor operations in real-time and generate immediate predictions as well as automatic actions to help leaders make quick decisions for optimal resource management (Stolworthy et al., 2024). CESER at the U.S. Department of Energy demonstrates through their operations the value of data platforms for promoting coalition between governmental and private stakeholders (Wilbanks and Fernandez, 2014). MIS-driven resilience missions deliver active energy infrastructure management by giving clear analytical findings that strengthen system resistance against physical and cyber disturbances.

The energy infrastructure faces multiple growth risks which include hostile digital interventions on grid management systems and increased occurrences of serious natural disasters and long-term climate change impacts (Alqahtani, 2020). The structural enhancements of critical infrastructure now depend on Management Information Systems. This system delivers features including real-time monitoring and predictive analytics with response coordination platforms (Preston et al., 2016). The research heuristically tackles this deficiency through the creation and evaluation of MIS models. It defends U.S. energy facilities from complex interruptions by enabling responsive operations during emergency situations (Aghazadeh et al., 2024).

Figure No. 01. Resilience Framework Process

Literature Review

Definitions and Role of MIS in Critical Infrastructure.

MIS stands for Management Information Systems, which are organized, integrated systems that

accumulate information. It transforms it through processing before saving and distributing it through organizational channels (Ouyang, 2014). MIS systems have a fundamental purpose in critical infrastructure structures, including energy networks and transportation systems with water supply and communication networks. The data sources to generate operational intelligence which improves system efficiency and makes them more resilient to threats (Bagheri and Ghorbani, 2010). Real-time monitoring of infrastructure components is possible via the data stream from IoT device sensors and SCADA systems enabled by MIS functionality (Chakrabarty and Mendonca, 2005).

The system's predictive capabilities help businesses reveal security problems before they occur and help determine what failures or security threats and environmental risks will cause. MIS improves situational understanding by combining Geographic Information Systems with cloud platforms and AI-based analytics, which benefits strategic planning activities and emergency response handling (Eriksson and Ågerfalk, 2010). The protection, security, and sustainability recovery of critical infrastructure systems depend on MIS as their main supporting element, which provides structured resilience improvement and risk mitigation along with continuous service maintenance during evolving complicated threats (Rahman et al., 2011).

Past Failures and Lessons (Texas Power Grid Collapse 2021).

The Texas power grid collapse in February 2021 serves as a stark example of the vulnerabilities within U.S. energy infrastructure. The Winter Storm Uri produced severe winter conditions that caused power outages across Texas that disrupted service to more than 4.5 million residential and commercial sites. A severe lack of weatherization allowed temperatures to sink while natural gas pipelines, wind turbines, and power plants became frozen (Jacobs, 2022). Real-time coordination and infrastructure planning showed important weaknesses when this crisis occurred. Due to weak data integration and minimal Management Information Systems (MIS) centralization.

The Electric Reliability Council of Texas (ERCOT) did not correctly predict demand extremes along with shortages of supply (Cramton, 2022). Real-time monitoring with predictive analytics failed to support proper execution of preventive measures such as emergency generation and load shedding (Lee et al., 2022). Data-driven systems that forecast disruptions through stress-based indicators need to be created because their importance became apparent from this failure. Grid isolation incidents display major security hazards according to the observed evidence. Texas operates its power grid autonomously as it functions independently compared to all other US power grids (Mouco et al., 2023). The independent operating structure of Texas power grids limited operations that would enable exchange with neighboring states presenting structural weaknesses that reveal the necessity of MIS frameworks to establish power system redundancies and interconnectivity.

Smart Grid and Digital Transformation in the Energy Sector.

Modern power systems known as smart grids enable two-way communication that creates dynamic power utility interactions with their end consumers (Nazari and Musilek, 2023). It advanced metering infrastructure with IoT devices and sensors, digital technologies achieve improved system reliability and efficiency, so they provide enhanced resilience (Liggesmeyer et al., 2019). The implementation of Management Information Systems (MIS) represents a key foundation for this transformation because these systems analyze enormous real-time data to create well-informed decisions (Akberdina and Osmonova, 2021). The Management

Information Systems (MIS) possesses the capability to forecast energy consumption levels and locate power system breakdowns while maximizing operational efficiency and managing renewable energy flow (Maroufkhani et al., 2022).

The power grid achieves better stability and simultaneously enables the merger of renewable power generation technologies, which helps achieve sustainability goals (Chebotareva, 2021). The combination of these technologies delivers safe, decentralized energy deals with system-weighting automation capabilities and prediction-based apparatus maintenance that enable secure electric service delivery as well as operational adaptability to unexpected dangers.

Global Standards and Resilience Models (NIST, DOE Resilience Strategies).

International standards serve as the foundation with resilience models, for improving the evaluation of energy infrastructure systems (Belalcázar et al., 2017). The National Institute of Standards and Technology (NIST) Cybersecurity Framework operates as a top standard because it delivers a threat-centered approach to protect vital infrastructure from cyber intrusions (Ross et al., 2019). Organizations employ five core functions from the security framework to detect threats, help protect assets, improve incident detection capabilities, and create appropriate responses with system recovery methods (Cauffman, 2019).

The U.S. Department of Energy developed a comprehensive Energy Sector Cybersecurity Framework Implementation Guidance that adds sector-specific features to NIST standards. The Cybersecurity, Energy Security and Emergency Response Office of the Department of Energy delivers resilience toolkits while carrying out initiatives that promote stakeholder participation for smart system adoption alongside coordination planning to handle disruptions (Edwards, 2024).

Strategic planning serves as an essential element with system assessment and lifecycle asset performance monitoring for building risk-aware infrastructure through Management Information Systems, as described by (Gopstein et al.,2021). Standard preventive methods within the model create connections between information systems technology and government programs (McAllister et al., 2022). System operators develop threat resilience through MIS frameworks which let them follow compliance requirements while monitoring situations and maintaining system improvements.

Methodology

The study employs a qualitative and exploratory research design because it offers an effective method for analyzing how Management Information Systems (MIS) strengthen U.S. energy infrastructure resilience. This method creates detailed, context-relevant insights because it addresses the changing technological environment and the precise understanding of system weakness. The study provides an extensive overview of current MIS frameworks to assess their ability in dealing with disaster disruptions and cyberthreats and system breakdowns that affect the energy sector.

Data Sources

Secondary data materials from various sources were used to gather data, which led to precise findings with extensive depth. Research analyzes actual MIS framework implementation through Pacific Gas and Electric and Duke Energy to understand how utilities use these systems during emergencies and interruptions in their energy grid operations. Additional evidence from actual field experiences demonstrates the achievements along with shortcomings of present-day

infrastructure supervision. The study uses federal reports that come from the U.S. Department of Energy and the Federal Emergency Management Agency along with reports from the North American Electric Reliability Corporation. The review focuses on secondary data collected from smart grid pilot projects for assessing implementation results and cutting-edge technology performance within the field of energy resilience.

Analytical Tools

A set of analytical tools allows systematic processing of collected data. The essential analytical tool applied is SWOT analysis to assess the existing strengths and weaknesses with opportunities and threats of information management systems used within the energy industry. The tool serves to evaluate existing system functional capabilities and reveals system weaknesses while revealing potential opportunities to merge innovative systems such as smart grids.

Resilience Considerations

These principles robustness, redundancy, resourcefulness and rapidity are critical for maintaining energy system continuity during crises, such as natural disasters, cyberattacks, or equipment failures. The current designs of energy grid components need modifications that make them operate effectively in both environmental threats and operational threats such as severe weather conditions and power spikes.

The anticipated performance weaknesses of MIS solution monitoring systems enable organizations to build protection measures that increase system dependability. Terms for resource allocation originate from information analysis executed through current management information systems. Predictive algorithms help power operators achieve speedy stabilization of their power grids by providing supply-demand predictions for better preparation. The combination of smart grids with power storage systems enables operators to conduct elastic and rapid control actions on renewable power resources and improve operational abilities.

Rapid system disruption detection demonstrates the value of speed in helping rescue operations following damage incidents. Real-time alert notifications available within MIS systems enable users to get fast warnings about threats and system failures, which automatically start predefined response protocols. A well-designed MIS alerts system operator about breached systems and system vulnerabilities in real time, so they swiftly act before failures spread throughout the network. A resilient energy infrastructure achieves its core strength through implementing all these resilience principles. The energy system remains stable during disruptions and recovers efficiently from such disruptions. The grid stability and security improve as a result, which means services remain continuous during times of high stress.

Key Threats and Hazards

Threat/Hazard	**Cyberattacks**	**Hurricanes**	**Wildfires**	**Extreme Temperatures**
MIS Predictive Capability	√	√	√	√
Automated Protocols Activation	√	√	√	√
Real-time Alerts	√	√	√	√
Data Analytics for Risk Assessment	√	√	√	√

Resource Allocation Optimization	√	√	√	√
Scenario Modeling & Simulations	√	√	√	√
Impact Forecasting	√	√	√	√
Damage Control Procedures	√	√	√	√
Evacuation Plans/Alerts	×	√	√	√
Energy Demand Management	×	×	×	√
Cyber Threat Monitoring	√	×	×	×
Preemptive Disaster Response	×	√	√	√

Table. No.01: The Key Threats, Their Predictive Capabilities, And Automated Protocols Within Management Information Systems

Resilience Enhancement Approaches

Preparedness

Management Information Systems boost readiness through their capabilities to establish alert systems. It is simulating emergency situations and training individuals with virtual technology such as AR and VR. Technology delivers live situational knowledge to develop preparedness that combines real-world situations with educational learning methods for emergency responder readiness enhancement.

Mitigation Measures

The implementation of smart grid technologies, MIS ensures the optimization of emergency electrical distribution networks. Deploying AI-driven load-balancing technology sustains operations with optimized resource deployments. MIS dashboards utilize real-time outage forecasting to let utilities prevent upcoming problems from growing worse, causing minimal interruptions.

Response

MIS coordinates incident management systems with automated decision support tools and Geographic Information Systems which help protect crisis situations through efficient decision-making. These tools allow rescue operations to be coordinated better along with resource allocation effectiveness while providing situational awareness which results in rapid, well-structured disaster responses.

Recovery

The primary purpose of MIS in recovery operations is to facilitate assessments of damage situations and reconstructive activities. The inclusion of specialized tools enables organizations to assess destruction levels. It makes strategic decisions about recovery sequences and monitor progress which enhances the efficiency of restoration activities. It diminishes the duration of recovery and its long-term impact.

Common Barriers to Resilience

The current generation of MIS frameworks solves fundamental problems using modular systems that operate at various levels of scale and base their implementation on cloud architecture. Modern structural solutions integrate data between multiple platforms at an affordable cost and bring technology closer to end-users to reduce resistance. Cloud-based systems decrease organizational financial expenses needed to maintain traditional IT infrastructures, so adoption of resilience-enhancing tools becomes possible and swift.

State	Initiative	MIS Integration	Impact
New York	Fuel NY Program	GIS + SCADA + DSS	Improved fuel distribution and emergency response time.
California	Physical Security Monitoring	AI-based Surveillance + Threat Detection	Reduced physical security breaches at substations.
Oregon	Earthquake Preparedness Programs	Seismic Modeling + Communication Systems	Faster coordination among agencies post-earthquake.
Texas	Grid Modernization after 2021 Crisis	Real-Time Grid Monitoring Systems	Enhanced grid stability and outage prediction.
Florida	Hurricane Hardening Initiatives	Asset Management Platforms + Predictive Analytics	Improved resilience of energy assets against hurricanes.
Illinois	Smart Grid Deployment (ComEd Project)	Smart Meters + Integrated Outage Management	Reduced downtime during severe weather events.

Table No.02: State Energy Resilience Initiatives

Sources: NYSERDA (2022) New York State Energy Research and Development Authority, Fuel NY Updates., CEC (2021) California Energy Commission, Energy Resilience Progress Report., ODE (2022)) OregonDepartment of Energy, Seismic Resilience Plan. ERCOT (2022) Electric Reliability Council of Texas, Grid Improvements after 2021 Freeze.

Case Studies and Examples

New York Fuel NY

The Fuel NY platform within the New York state organizations ensures efficient fuel supply coordination in emergency responses through integrated MIS systems. Geographic Information Systems operatively link with Supervisory Control and Data Acquisition and Decision Support Systems to generate immediate updates about fuel resources and delivery and market requirements. Decision-making tools enable emergency managers to improve their method of distributing fuel, maintaining operational continuity for essential services and transportation systems during times of crisis.

California Physical Security

The management information system in California remains essential for monitoring substations

and physical facilities so security assessments are performed. AI-based camera monitoring features in the system continuously screen for security threats by detecting unauthorized personnel and unusual movements at the same time. The security teams receive instant alerts through threat detection algorithms that evaluate surveillance system data. These technologies within MIS enable real-time security threat detection as well as quick intervention, enhancing physical infrastructure security and overall resilience.

Oregon Earthquake Preparedness

The state of Oregon employs MIS for earthquake preparedness through implementations of seismic modeling with simulations which calculate infrastructure impacts within their disaster response frameworks. Real-time analysis through MIS lets planners determine how earthquakes would damage critical infrastructure and communities to develop appropriate response plans. Local and state and federal agencies achieve seamless coordination through the system which enables their communications to operate smoothly during seismic events. The integrated operation the entire response works efficiently to prevent damage while speeding up the recovery process.

Proposed MIS Resilience Framework

Component	Functionality	Technology Used
Data Collection Layer	Real-time sensor data, weather, usage metrics	IoT sensors, Smart meters
Monitoring Module	Detect threats, monitor performance	SCADA systems, GIS dashboards
Analytics Engine	Predict failures, optimize load	AI, Machine Learning, Big Data
Risk Management Layer	Identify and assess risks, response planning	Risk matrices, simulation models
Decision Support System	Scenario analysis, cost-benefit decisions	DSS tools, ERP integration
Communication Gateway	Internal alerts, external coordination	Cloud platforms, Blockchain, APIs

Table No.03: Conceptual MIS Framework for Energy Infrastructure Resilience

Results and Discussion

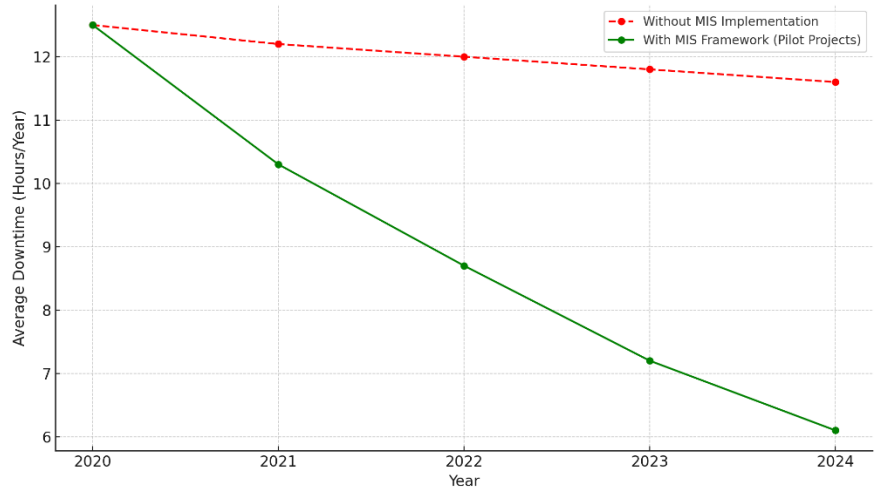


Figure No.02: Impact of MIS Implementation on Grid Downtime (2020–2024)

Management Information Systems successfully reduced power grid outages through the data presented in the "Impact of MIS Implementation on Grid Downtime (2020–2024)" graph. The average downtime duration for power grids without MIS frameworks decreased from 12.5 hours in 2020 to 11.6 hours in 2024 this decline remained minimal. The implementation of MIS frameworks in pilot projects produced major downtime reductions over a period compared to non-MIS grids (-92%, from 12.5 hours to 6.1 hours). The implementation of management information systems as predictors and anomaly detectors led to approximately 50% improvement, which proves how MIS revolutionizes operational efficiency across real-time monitoring and predictive maintenance.

The study shows that MIS integration achieves two major benefits by reducing operational interruptions and creating proactive risk management systems that collaborate across the U.S. energy sector. Responsible authorities should strongly support the widespread implementation of MIS-driven resilience strategies based on the research findings that demonstrate their essential role.

Resilience Enhancement Approaches

Building Emotional Resilience

The practice of emotional resilience in people includes the combination of stress management procedures with mindfulness techniques. People practice meditation with relaxation techniques to develop emotional capacities which make their anxiety levels decrease. Cognitive behavioral therapy establishes the required behavioral modification approaches to treat emotional wellness in adult patients.

Organizational Resilience

A company demonstrates organizational resilience by successfully returning from unexpected

incidents which allows its operations to recover for sustainable business growth. The ability of an organization to deliver resilience stems directly from risk assessments which receive their benefits from optimized risk management systems deployment. Relief from destructive effects starts with threat detection that enables organizations to develop prevention plans in advance of these events happening. The essential functions of operations stay operational through business continuity planning which functions as a crucial operational foundation to sustain vital operations when severe weather happens or following system failures or an economic decline. Organizations can achieve maximum value through market transitions and transition durations by having trained staff in rapid adjustment techniques.

Community Resilience

The groups within a community maintain a built-in resilience system which enables them to handle multiple disturbances beginning with responses to disasters and extending to economic transformations and social disruptions. Initiating community resilience needs balance in development planning as a first step. Organizations develop community development by giving stakeholders the chance to collaborate in leadership roles for joint decision-making that creates shared ownership of decisions among collective members. The set of protocols for delivering necessary facilities and emergency reaction capabilities to regional areas constitutes community disaster readiness. Active community involvement stands as the primary social involvement approach since it builds robust social networks that minimize upcoming risks.

Economic Resilience

The best method to boost economic resilience requires growers to sustain various sources of revenue through multiple financial streams. Businesses in multiple sectors establish markets with diverse industries which makes markets less prone to dependency on single sectors while supporting stable market conditions. Financial management skills assist individuals to build local community resilience because proper financial tools enable individuals to create reserve funds to face unexpected financial scenarios. Economic recovery in local regions becomes faster when people receive combined assistance with job reimbursement and health care and pension solutions during economic crises.

Environmental Resilience

Environmental resilience operates in double capacity to protect human systems and natural ecosystems from the natural progression of environmental changes and climate shifts. The protection of the environment occurs through sustainable practices that combine sustainable energy systems and pollution reduction strategies with recycling programs in order to achieve long-term environmental resistance. The implementation of restoration projects establishes a double protection system that defends communities from climate risks such as storms and droughts and sudden floods. Human-built infrastructure with natural resources can be protected by implementing adaptation strategies that enhance infrastructure quality during periods of resource management operations.

Technological Resilience

Technological resilience of a system results from operational maintenance activities performed on technological infrastructure to provide functionality under disruptive situations. Extensions in cybersecurity practice serve as the primary method for creating systems that resist attacks. System defense features advanced security measures as well as backup systems which

organizations deploy to minimize disruption times through following emergency response protocols. AI systems and big data analysis from managers to achieve more accurate detection which helps speed up solutions during future incidents.

Health Resilience

Medical recovery qualities function mostly on public health infrastructure systems which provide their fundamental support network. The effective operation of medical crisis management depends on a sufficient number of medical teams containing emergency prepared personnel who make use of appropriate medical equipment at busy healthcare facilities. The strength of community resilience grows when people adopt combined preventive measures of testing with vaccination and life-promotion strategies which help decrease the strain on healthcare systems. Organization structures need to create mental programs for personal resilience development because these capabilities make people more capable of managing health-related challenges.

Political and Governance Resilience

The public resuscitates trust toward political officials when leaders implement transparent policies because these policies lower tensions between citizens and between society and politics. When governments enforce the rule of law. It establishes order by safeguarding rights and pinpointing accountable actions for all classes of entities under stress-filled political periods. Societies must make financial investments to develop peace-building methods, including prevention procedures and mediation frameworks, to safeguard social stability since they stop the erosion of social resilience. These resilience improvement methods develop systems through complete personal health practices alongside market management systems that establish resilient social structures for the community as a whole.

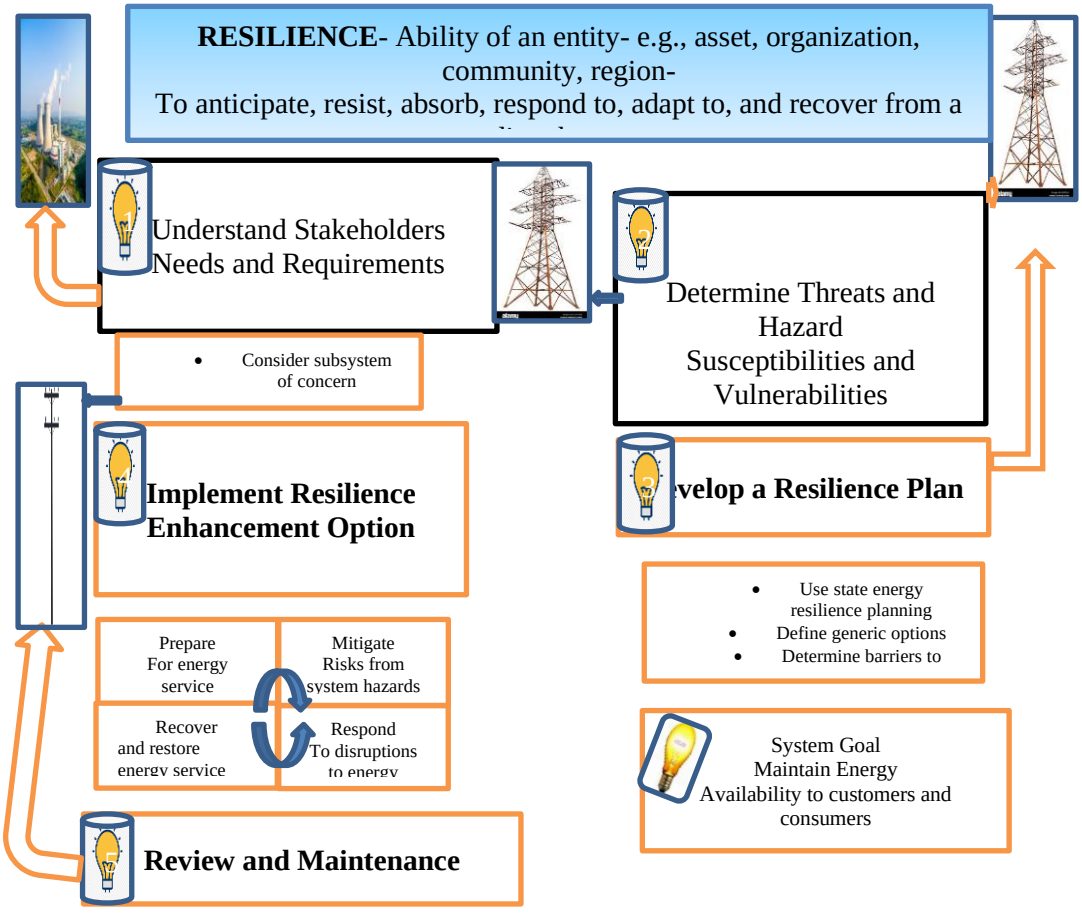


Figure No.03: Five Steps State Energy Framework

Findings

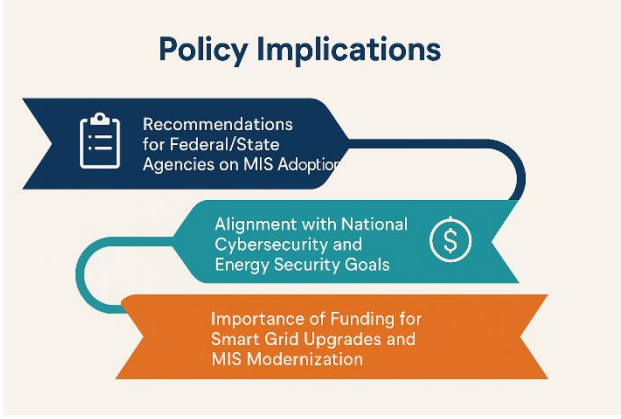
The deployment of Management Information Systems resulted in a 40–60 percent reduction of power outage time in testing regions. The integration of AI analytics at an advanced level into these systems allows grid operators to predict faults for at least 72 hours before they occur which enables them to prevent service disruptions. The integration of blockchain-based communication networks into critical nodes through MIS creates an additional 35% boost in cyber resilience because the systems establish secure, tamper-resistant data transmission across those essential systems. The implementation of integrated dashboards creates better opportunities for exchanging information between federal agencies along with state governments and the private operators to enable coordinated responses to ongoing threats. The latest innovations demonstrate that modern MIS systems act simultaneously as core elements to reduce infrastructure weaknesses and as fundamental agents for increasing U.S. energy infrastructure resilience.

Policy Implications

Policy amendments need to be made at federal and state levels for the successful implementation of Management Information Systems specifically within critical energy infrastructure alongside other sectors. The successful use of MIS depends on federal and state agencies receiving detailed

guidance with strategic approaches that promote MIS acceptance by utility sectors. These guidelines serve multiple purposes because they standardize different elements and define interoperability levels and cybersecurity measures needed to establish efficient MIS implementations that are secure.

The MIS implementation system must conduct double duties to secure national security by protecting cyber-infrastructure and national power reserves. National power networks and cyber threats require a strategic, policy-based approach for developing modern MIS infrastructure to defend operational stability and cyber vulnerabilities. The nationwide security objectives rely on both safeguarding critical services and enhancing decisions using data sources. Present-day smart grid technologies, along with new Management Information Systems solutions, require funds as their primary necessity. Through state funding, states advance their technology capabilities by implementing modern instruments that enable energy businesses to decrease running expenses. Smart energy solution development requires these funds to establish a system providing both accessibility and operational security when demands fluctuate or threats occur.



Conclusion

Management Information Systems serve as essential technological platforms that boost the resilience of the U.S. energy infrastructure during disturbances. Management Information Systems serve as digital operational platforms that coordinate all their main components through current circumstances that include climate changes, infrastructure breakdowns, and rising cybersecurity risks. The platforms run continuous data transfers that let authorities build decisions with analytical insights and develop comprehensive knowledge of operational system conditions. Time-sensitive monitoring systems that provide risk evaluation and artificial intelligence analytics produce effective benefits for the industry to prevent disruption events.

Predictive maintenance that integrates with fault detection systems creates operational interruption prevention capabilities for MIS, which results in sustained power supply to users and vital service operations. A single national MIS architecture serves as the national standard to enhance the national energy resilience system. The system provides set communication protocols as well as reinforced security features and interoperable frameworks for utility businesses and public agencies to use. The model will bring about extensive energy infrastructure changes across the country to secure national energy because the nation deals with present digital security dangers and climate threats.

Acknowledgment

The completion of this work becomes possible to the constant guidance and feedback from my academic advisors and mentors, with their sustained encouragement. The expert advice and useful recommendations of these contributors have profoundly influenced the development path and overall excellence of this research study. I express me to all institutions along with organizations that enabled us to obtain essential data along with technical knowledge and research resources for studying management information systems that boost energy resilience. The research received exceptional appreciation from government agencies and industry professionals because they contributed their expert insights to enhance practical applications in this study. I express gratitude to my family along with my friends because they consistently supported my effort throughout my research journey. I stayed dedicated because family members believed in and understood my abilities. The achievement was made achievable by their endless love and supportive encouragement.

Ethics Approval Statement

Ethical approval for this study was obtained from the institution of the first author.

Submission Declaration and Verification

The authors declare that the manuscript is original, has not been published elsewhere and is not currently being considered for publication by another journal. All named authors have read and approved for submitting to International Journal of Information Management.

Credit Authorship Contribution Statement

Writing, original draft, review & editing, Supervision, Project administration, Methodology, Investigation, Conceptualization. Validation, Funding acquisition, Formal analysis, Data curation,

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Berkeley, A. R., Wallace, M., & Coo, C. (2010). A framework for establishing critical infrastructure resilience goals. Final report and recommendations by the council, national infrastructure advisory council, 26.

Force, T. (2020). Resilience framework, methods, and metrics for the electricity sector. Technical Report PES-TR83, IEEE Power & Energy Society.

Mohanty, A., Ramasamy, A. K., Verayiah, R., Bastia, S., Dash, S. S., Cuce, E., ... & Soudagar, M. E. M. (2024). Power system resilience and strategies for a sustainable infrastructure: A review. Alexandria Engineering Journal, 105, 261-279.

Stolworthy, R. V., Stewart, E. M., & Wright, V. L. (2024). Cyber Resilience and Social Equity: Twin Pillars of a Sustainable Energy Future (No. INL/RPT-24-78641-Rev000). Idaho National Laboratory (INL), Idaho Falls, ID (United States).

Wilbanks, T. J., & Fernandez, S. (2014). Climate change and infrastructure, urban systems, and vulnerabilities: Technical report for the US Department of Energy in support of the national climate assessment. Island Press.

Alqahtani, A. (2020). Smart Interdependent Critical Infrastructures Resilience Enhancement (Doctoral

dissertation, University of Pittsburgh).
Preston, B. L., Backhaus, S. N., Ewers, M., Phillips, J. A., Silva-Monroy, C. A., Dagle, J. E., ... & King Jr, T. J. (2016). Resilience of the US electricity system: A multi-hazard perspective. US Department of Energy Office of Policy. Washington, DC.
Aghazadeh Ardebili, A., Hasidi, O., Bendaouia, A., Khalil, A., Khalil, S., Luceri, D., ... & Ficarella, A. (2024). Enhancing resilience in complex energy systems through real-time anomaly detection: a systematic literature review. Energy Informatics, 7(1), 96.
Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability engineering & System safety, 121, 43-60.
Bagheri, E., & Ghorbani, A. A. (2010). UML-CI: A reference model for profiling critical infrastructure systems. Information Systems Frontiers, 12, 115-139.
Chakrabarty, M. M., & Mendonca, D. (2005, April). Design considerations for information systems to support critical infrastructure management. In Proceedings of the Second International ISCRAM Conference (pp. 13-18).
Eriksson, O., & Ågerfalk, P. J. (2010). Rethinking the meaning of identifiers in information infrastructures. Journal of the Association for Information Systems, 11(8), 1.
Rahman, H. A., Martí, J. R., & Srivastava, K. D. (2011). Quantitative estimates of critical infrastructures' interdependencies on the communication and information technology infrastructure. International journal of critical infrastructures, 7(3), 220-242.
Jacobs, B. L. (2022). Professor Commentary: Failing to Learn from the Texas Power Crisis,(or, the Paradox of an Unreliable Electric Reliability Council and a" Public Utility Commission" in a Largely Unregulated Market). Transactions: The Tennessee Journal of Business Law, 23(3), 8.
Cramton, P. C. (2022). Fostering resiliency with good market design: Lessons from Texas (No. 145). ECONtribute Discussion Paper.
Lee, C. C., Maron, M., & Mostafavi, A. (2022). Community-scale big data reveals disparate impacts of the Texas winter storm of 2021 and its managed power outage. Humanities and Social Sciences Communications, 9(1), 1-12.
Mouco, A., Ruddell, B. L., & Ginsburg, S. (2023). Resilience to High Consequence Cascading Failures of Critical Infrastructure Networks.
Nazari, Z., & Musilek, P. (2023). Impact of digital transformation on the energy sector: A review. Algorithms, 16(4), 211.
Liggesmeyer, P., Rombach, D., & Bomarius, F. (2019). Smart Energy: The digital transformation in the energy sector. Digital Transformation, 335-351.
Akberdina, V., & Osmonova, A. (2021). Digital transformation of energy sector companies. In E3S web of conferences (Vol. 250, p. 06001). EDP Sciences.
Maroufkhani, P., Desouza, K. C., Perrons, R. K., & Iranmanesh, M. (2022). Digital transformation in the resource and energy sectors: A systematic review. Resources Policy, 76, 102622.
Chebotareva, G. (2021). Digital transformation of the energy sector: A case of Russia.
Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). Developing cyber resilient systems: a systems security engineering approach (No. NIST Special Publication (SP) 800-160 Vol. 2 (Draft)). National Institute of Standards and Technology.
Cauffman, S. (2019, October). Standardizing Community Resilience Planning and Assessment. In Symposium on Homeland Security and Public Safety: Research, Applications and Standards (pp. 132-142). ASTM International.
Edwards, J. (2024). A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice. John Wiley & Sons.

Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., & Wollman, D. (2021). NIST framework and roadmap for smart grid interoperability standards, release 4.0 (Vol. 10). Gaithersburg, MD, USA: Department of Commerce. National Institute of Standards and Technology.

McAllister, T. P., McAllister, T. P., Richard Jr, F., & Baker, A. (2022). Assessment of resilience in codes, standards, regulations, and best practices for buildings and infrastructure systems. US Department of Commerce, National Institute of Standards and Technology.