Journal of Economics, Finance and Management Studies

ISSN (print): 2644-0490, ISSN (online): 2644-0504

Volume 08 Issue 07 July 2025

Article DOI: 10.47191/jefms/v8-i7-27, Impact Factor: 8.317

Page No: 4337-4350

The Impact of AI-Based Predictive Maintenance and Demand Response Integration on Smart Grid Operational Efficiency: The Moderating Role of Cybersecurity Readiness

Nguyen Thi Kim Phung[1], Do Hoang Dung[2]

[1]Faculty of Business Management, University of Greenwich, UK

[2]Nguyen Khuyen high school, HCM, Vietnam,

ABSTRACT: This study examines the influence of demand response integration and AI-based predictive maintenance on smart grid operational efficiency, with an emphasis on the moderating effect of cybersecurity readiness. Based on the theories of contingency and socio-technical systems, the study views smart grid efficiency as a result of both institutional readiness and technological innovation. Using a 5-point Likert scale, a quantitative survey was given to 385 professionals working in the cybersecurity and energy industries in Vietnam. The results show that demand response integration ($\beta = 0.508$) and AI-based predictive maintenance ($\beta = 0.635$) both considerably improve operational efficiency. Additionally, the association between AI-based maintenance and efficiency was shown to be moderated by cybersecurity preparedness ($\beta = 0.472$), indicating that digital protection procedures are necessary to benefit from predictive technology fully. By experimentally connecting cybersecurity with smart grid functioning, the study closes a significant gap in the literature and offers a comprehensive paradigm for resilient energy modernization. The findings provide useful information for engineers, legislators, and energy companies attempting to strike a balance between risk reduction and innovation in digitalized energy ecosystems.

KEYWORDS: Smart grid efficiency; demand response integration; AI-based predictive maintenance; cybersecurity readiness.

1. INTRODUCTION

The research problem addresses the challenges of digital transformation in the energy sector, specifically within the domain of smart grids, by examining the role of AI-based predictive maintenance and demand response integration in enhancing operational efficiency. In recent years, the global transition to smart energy systems has intensified, with smart grids viewed as a critical infrastructure to optimize electricity distribution and maintain energy security (Almeida *et al.,* 2025). While the implementation of Artificial Intelligence (AI) enables predictive diagnostics and proactive asset management, its success is contingent on the grid's cybersecurity posture (Alcaraz & Zeadally, 2015). Similarly, demand response mechanisms can facilitate load balancing and cost savings, but their reliability and effectiveness hinge on secure and stable data exchange networks (Luthra *et al.,* 2013).

The growing digitization of grid operations introduces new vulnerabilities, with cybersecurity readiness emerging as a pivotal factor moderating the technological benefits derived from AI and demand response integration (Li *et al.,* 2010). Despite these developments, the extant literature often isolates technological factors without addressing the interconnected impact of cybersecurity readiness—a gap this study aims to fill. The significance of integrating AI and demand response with robust cybersecurity systems is underscored by increasing reports of cyber threats targeting critical infrastructure (Hasegawa *et al.,* 2024), highlighting the urgent need for coordinated digital and security strategies.

Previous research has tended to focus on the standalone impacts of AI or demand response in developed markets, often overlooking the combined influence of these technologies under varying levels of cybersecurity preparedness, especially in contexts where cyber threats are rapidly evolving (Hashem *et al.,* 2015). Furthermore, existing models lack a unified framework that encapsulates these technological and institutional variables to offer a comprehensive view of smart grid performance (Yin *et al.,* 2015). This study addresses these gaps by proposing an integrative model that considers the dual impact of AI-based predictive maintenance and demand response integration on operational efficiency, with cybersecurity readiness acting as a moderating variable.

The overarching research questions for this study are:

1. What is the impact of AI-based predictive maintenance on smart grid operational efficiency?
2. How does demand response integration influence grid performance in a digitalized energy ecosystem?
3. How does cybersecurity readiness moderate the relationship between AI-based predictive maintenance and smart grid operational efficiency?

Guided by these research questions, the study has three core objectives. First, to examine the direct impact of AI and demand response on smart grid efficiency. Second, to evaluate how cybersecurity readiness enhances or undermines these technological applications. Third, to provide a theoretical and practical framework for policymakers, energy firms, and engineers seeking to ensure secure, resilient, and efficient grid modernization.

2. LITERATURE REVIEW

2.1. Smart grid operational efficiency

Smart grid operational efficiency refers to the capacity of a digitally enhanced power grid to deliver electricity in a secure, cost-effective, and environmentally sustainable manner through the integration of advanced technologies such as artificial intelligence (AI), automation, predictive maintenance, and demand response systems (Fatima & Arshad, 2025). This concept captures the grid's ability to optimize energy flow, reduce transmission losses, extend asset lifespan, and enhance service reliability through real-time monitoring and data-driven decision-making (Fang *et al.,* 2011). At its core, smart grid efficiency involves minimizing system downtimes, improving fault detection and recovery processes, and balancing supply-demand dynamics more effectively, especially during peak load periods (Siano, 2014). The growing role of AI-based predictive maintenance, for instance, allows for proactive asset management by identifying faults before they occur, reducing the frequency and severity of outages, and enhancing the overall resilience of grid infrastructure (Zhou *et al.,* 2016). Similarly, the integration of demand response strategies enables the dynamic adjustment of electricity consumption, fostering more balanced grid operations and greater energy conservation (Gyamfi *et al*., 2013). Despite these technical advancements, achieving operational efficiency in smart grids also requires institutional coordination, adequate policy frameworks, and a well-prepared cybersecurity posture to safeguard digital systems from potential threats (Güngör et al., 2011).

To better understand the multidimensional nature of smart grid performance, two theoretical perspectives provide critical insight: Socio-Technical Systems Theory (STST) and Contingency Theory. STST views the smart grid as a complex system where technological infrastructure and human-social elements must be jointly optimized to ensure performance (Trist, 1981). Within this framework, the effectiveness of AI tools, for example, is closely tied to operator readiness, organizational culture, and stakeholder collaboration (Büscher & Sumpf, 2015). Contingency Theory complements this view by emphasizing that the performance of smart grid systems depends on their ability to align internal capabilities with external contextual factors such as regulatory environments, infrastructure maturity, and cybersecurity readiness (Donaldson, 2001). These theoretical lenses underscore that smart grid operational efficiency is not solely a product of technical advancement but rather the result of continuous adaptation to evolving socio-technical conditions. Especially in emerging economies, where digital infrastructure and institutional capacity may be underdeveloped, applying both theories enables a more holistic understanding of the barriers and enablers shaping smart grid transformation. Therefore, improving smart grid operational efficiency necessitates a systemic approach that integrates technical innovation with human-centered design and responsive policy mechanisms.

2.2. Critical Analysis of Theoretical Frameworks

This study adopts Socio-Technical Systems Theory (STST) (Trist, 1981) and Contingency Theory (Donaldson, 2001) to critically examine the interplay between emerging technologies and operational efficiency in smart grids, with a particular focus on the moderating role of cybersecurity readiness. STST emphasizes the co-evolution of social and technical subsystems within complex organizational environments, underscoring that smart grid performance depends not only on technological sophistication but also on the readiness and adaptability of human and institutional actors (Cherns, 1987). In the context of smart grids, AI-based predictive maintenance and demand response strategies can only deliver optimal results when integrated into socio-technical infrastructures that align with organizational culture, user capabilities, and stakeholder coordination (Büscher & Sumpf, 2015). Complementing this, Contingency Theory posits that there is no one-size-fits-all solution to system optimization, and the effectiveness of smart grid interventions depends on how well they align with contextual variables such as regulatory stability, market structures, and cybersecurity preparedness (Güngör *et al.,* 2011). This framework is particularly relevant in emerging economies where smart grid deployment occurs in rapidly changing environments marked by institutional fragmentation and digital insecurity. The integration of STST and Contingency Theory allows for a nuanced understanding of smart grid operational efficiency as a dynamic outcome shaped by the interdependence between technical innovation and socio-organizational alignment. By accounting for the reciprocal influences between system design, institutional arrangements, and contextual volatility, these frameworks collectively illuminate the critical pathways through which smart grids can achieve resilient, efficient, and secure digital transformation.

2.2.1. Socio-Technical Systems Theory

The Socio-Technical Systems Theory (STST), introduced by Trist (1981), provides a foundational lens for understanding how technological innovations must be integrated within a broader social and organizational context to realize their full potential. At its core, STST posits that system performance emerges from the joint optimization of two interdependent subsystems: the technical system, comprising tools, technologies, and workflows, and the social system, encompassing people, culture, institutional norms, and governance structures (Cherns, 1987). Within the context of smart grid development, STST is especially relevant in examining how AI-based predictive maintenance and demand response strategies influence operational efficiency when implemented within socio-organizational structures that must also adapt and evolve. For instance, AI-driven predictive maintenance can enhance smart grid reliability by detecting faults before failures occur. Still, its effectiveness depends heavily on operator trust, employee digital competence, and organizational readiness to respond to algorithmic insights (Büscher & Sumpf, 2015). Similarly, the integration of demand response programs into grid operations requires not only technological infrastructure but also coordinated behavior from consumers, regulators, and utility providers, all of which are social components embedded within the energy system. STST highlights that technological adoption in the smart grid domain is not a purely technical endeavor—it involves managing change within complex social environments, fostering inter-agency collaboration, and aligning diverse stakeholder goals. Cybersecurity readiness, as a moderating factor, further emphasizes the socio-technical nature of the grid, requiring both robust digital defenses and an organizational culture of cyber-awareness and resilience. In emerging economies where institutional structures may be less mature, STST provides a robust framework to understand how human factors, governance, and system interoperability collectively shape the success of digital transformation in energy infrastructure. By incorporating both technological and human-centered considerations, STST enables a holistic assessment of how AI and demand response can be leveraged effectively and securely to enhance smart grid operational efficiency.

2.2.2. Contingency Theory

Contingency Theory, as articulated by Donaldson (2001), posits that there is no universally optimal approach to organizational design or technological implementation; rather, effectiveness is contingent upon the alignment between internal structures and external environmental conditions. This theory asserts that organizational success is achieved when there is a strategic fit between operational mechanisms and contextual variables such as technological complexity, regulatory frameworks, and market volatility. In the context of smart grid development, Contingency Theory provides a valuable framework for analyzing how AI-based predictive maintenance and demand response strategies affect operational efficiency, depending on the degree of cybersecurity readiness and institutional maturity. AI-driven maintenance technologies can significantly enhance grid reliability and efficiency through real-time fault prediction and proactive asset management, but their effectiveness varies depending on contextual factors such as cybersecurity infrastructure, regulatory support, and digital literacy among grid operators (Fatima & Arshad, 2025). Likewise, demand response integration requires adaptive grid protocols and user engagement, both of which must align with external contingencies, including energy market dynamics, policy incentives, and technological interoperability standards (Güngör *et al.,* 2011). In emerging economies, where institutional uncertainty and infrastructural deficits are common, the success of these technologies is highly contingent on the extent to which organizational capabilities and governance frameworks can absorb and adapt to digital disruptions. Cybersecurity readiness emerges as a critical moderating factor in this framework, as it influences the reliability and resilience of smart grid operations under AI- and data-driven conditions (Bostrom *et al.,* 2016). Contingency Theory thus underscores the importance of context-aware planning and the need for flexible system design that can be tailored to specific environmental demands. It highlights that the impact of advanced technologies on grid performance is not deterministic but conditional, varying according to the interplay between technological potential and institutional preparedness. Therefore, this theory offers a pragmatic and adaptive perspective, allowing policymakers and utility providers to calibrate smart grid strategies to fit local constraints and opportunities for achieving sustainable operational efficiency.

2.3. The Impact of AI-Based Predictive Maintenance on Smart Grid Operational Efficiency

AI-based predictive maintenance refers to the utilization of artificial intelligence techniques—particularly machine learning, deep learning, and real-time data analytics—to forecast the health and failure risk of infrastructure components. Within smart grid systems, this involves deploying algorithms that interpret sensor data, historical maintenance records, and performance patterns to anticipate malfunctions before they occur. This predictive capability enables utility providers to implement timely interventions, thus reducing downtime, extending asset lifespans, and enhancing overall operational efficiency (Lee *et al.,* 2015). By shifting from reactive and scheduled maintenance to condition-based and anticipatory strategies, AI-based predictive maintenance represents a foundational innovation in the management of complex, interconnected energy networks.

The application of AI-based predictive maintenance in smart grids marks a pivotal development in the digital transformation of the energy sector. Smart grids are designed to integrate advanced technologies to deliver electricity in a more reliable, resilient, and cost-effective manner. In this context, predictive maintenance powered by AI emerges as a key enabler of operational efficiency. It allows utilities to continuously monitor the condition of grid components, detect anomalies, and predict failures with a high degree of accuracy. This data-driven approach enables the timely replacement or repair of equipment, thereby minimizing unscheduled outages, optimizing asset utilization, and reducing maintenance costs (Mohammadi *et al.,* 2017).

The efficiency benefits of AI-based predictive maintenance are particularly critical in an environment characterized by increasing demand variability, decentralized generation, and growing system complexity. Empirical studies have highlighted that predictive maintenance can lead to significant performance improvements. For example, Wang *et al*. (2014) found that utilities employing AI-driven maintenance strategies experienced a 35% reduction in equipment downtime and a 25% extension in asset lifespan. These operational gains translate directly into economic and environmental benefits, as fewer failures mean lower repair costs, reduced energy losses, and less reliance on carbon-intensive backup systems.

From a philosophical standpoint, Technologism offers a compelling lens through which to understand the growing reliance on AI-based predictive maintenance. Technologism posits that technological innovation is not merely a support mechanism but a primary driver of societal and infrastructural progress (Feenberg, 2012). Within the smart grid context, predictive maintenance technologies are not passive tools but active forces shaping the evolution of energy systems. They reconfigure operational practices, institutional norms, and regulatory approaches by enabling unprecedented levels of foresight and automation. The intelligence embedded in these systems facilitates a transition from static, reactive grids to dynamic, responsive infrastructures capable of learning and adapting over time. This philosophical view underscores the transformative role of AI not only in improving system performance but in redefining what constitutes “efficiency” in energy delivery.

Complementing this perspective, Instrumentalism provides a practical and functional understanding of the role of AI in grid maintenance. Instrumentalism regards technology as a means to an end, valuable only insofar as it serves specific objectives (Heidegger, 1977). In the case of predictive maintenance, the end goal is clear: operational efficiency. AI systems are evaluated based on their ability to achieve measurable outcomes such as reduced downtime, optimized resource allocation, and increased grid reliability. Instrumentalism reminds us that the value of AI lies not in its novelty or complexity, but in its practical utility to stakeholders—from grid operators and energy firms to consumers and regulators. By enabling precise diagnostics and optimized maintenance schedules, AI fulfills its instrumental purpose, contributing directly to the resilience and effectiveness of the smart grid.

An important feature of this problem within the scope of the current research is its embeddedness within a complex socio-technical system. The effectiveness of AI-based predictive maintenance depends not only on algorithmic sophistication but also on the quality of data inputs, interoperability of devices, workforce readiness, and—critically—cybersecurity infrastructure. As outlined in the project framework, cybersecurity readiness serves as a moderating factor that conditions the success of AI applications. Without robust protections for data integrity and system access, predictive algorithms may produce unreliable outputs or fall victim to malicious interference, thereby compromising operational efficiency rather than enhancing it (Fang *et al*., 2011). Nonetheless, within a well-secured digital environment, AI-based predictive maintenance demonstrates a strong causal relationship with improved operational performance. It reduces the frequency and severity of outages, supports demand-side responsiveness, and facilitates proactive asset management. These advantages are central to the broader goals of energy sustainability and system resilience. Moreover, predictive maintenance supports long-term infrastructure planning by generating insights that inform capital investment and lifecycle management strategies. Thus, it contributes not only to immediate operational efficiency but to the strategic evolution of smart grids in response to future energy challenges.

Guided by the underlying theoretical framework, we establish the rationale leading to hypothesis one as follows:

H1: AI-based predictive maintenance has a positive impact on smart grid operational efficiency.

2.4. The Impact of Demand Response Integration on Smart Grid Operational Efficiency

Demand response integration refers to the systematic incorporation of demand-side energy management strategies into smart grid operations, wherein electricity consumers adjust their consumption patterns in response to real-time price signals, grid conditions, or external incentives. It enables utilities to balance supply and demand dynamically by encouraging load reductions or shifts during peak times, thereby enhancing grid reliability, economic efficiency, and sustainability. The integration of such mechanisms within smart grids is increasingly facilitated by digital technologies, including automated control systems, advanced metering infrastructure, and consumer-facing platforms (Palensky and Dietrich, 2011).

The integration of demand response (DR) strategies into smart grids represents a cornerstone of the energy sector's shift towards more adaptive, decentralized, and efficient systems. Operational efficiency in smart grids encompasses the grid's ability to deliver electricity reliably, cost-effectively, and sustainably while minimizing losses and maximizing flexibility. Within this context, demand response provides a powerful lever to modulate energy use in real time, alleviating stress on grid infrastructure, reducing the need for expensive peaking plants, and enabling better integration of intermittent renewable sources (Faruqui & Sergici, 2010). By aligning electricity demand more closely with supply, particularly during peak load periods, DR programs significantly improve the responsiveness and economic efficiency of grid operations.

Empirical evidence underscores the effectiveness of DR integration in improving grid performance. According to a study by Albadi and El-Saadany (2008), demand response measures in large-scale pilot programs across the United States and Europe led to a reduction in peak demand by up to 20%, resulting in considerable cost savings and enhanced reliability. Moreover, automated DR systems empowered by Internet of Things (IoT) and AI technologies can optimize these shifts in consumption in milliseconds, reducing latency and human error while enhancing system stability (Safari *et al.,* 2024). These features collectively contribute to the broader goal of operational efficiency by ensuring that energy is used where and when it is most needed, without requiring costly and carbon-intensive infrastructure expansion.

From a philosophical standpoint, the relevance of Pragmatism to demand response integration lies in its focus on actionable, results-oriented solutions to complex problems. Pragmatism emphasizes practical consequences and real-world effectiveness over theoretical ideals, which resonates with the core premise of DR systems: empowering consumers and operators to make real-time decisions that yield measurable improvements in grid performance (Dewey, 1929). Rather than prescribing rigid consumption rules, DR mechanisms provide flexible, decentralized responses based on real-time conditions, embodying the adaptive logic of pragmatist reasoning. This is particularly important in modern energy systems where variability—in both supply (e.g., renewables) and demand (e.g., electric vehicles, smart homes)—demands equally flexible solutions. Pragmatism affirms the value of DR not because it is technologically novel, but because it demonstrably enhances the grid's ability to function efficiently and reliably in diverse and changing conditions.

In parallel, Securitism (or Cybersecuritism) offers a critical lens through which to understand the challenges and imperatives associated with integrating demand response into digital grid infrastructures. As DR mechanisms rely on a dense web of communication technologies, including real-time data transmission between consumers and grid operators, they are inherently vulnerable to cyber threats. These threats include data manipulation, system hijacking, and unauthorized access, all of which can undermine grid stability and erode trust in digital energy systems (Liu *et al.,* 2024). From the securitist perspective, operational efficiency is not only a function of technical optimization but also of security assurance. A highly efficient demand response system that is vulnerable to cyber-attacks becomes a strategic liability rather than an asset. Thus, securitism reframes efficiency not as a purely technical outcome but as a socio-technical condition in which security and functionality must co-exist.

This perspective is especially pertinent in the context of smart grids, where the increasing sophistication of digital tools must be matched by a proportional commitment to cybersecurity governance. For instance, automated DR systems often require remote control of customer appliances and industrial equipment, making them attractive targets for cyber attackers. A successful intrusion could result in load imbalances, blackouts, or manipulation of electricity pricing signals—all of which directly compromise operational efficiency. Consequently, DR integration must be pursued alongside robust authentication protocols, secure data channels, and resilient system architectures to ensure that efficiency gains are not offset by increased exposure to cyber risks (Khurana *et al*., 2010).

A distinctive characteristic of this problem within the present project is the dual dependence of demand response on both consumer behavior and system-level coordination. Unlike hardware-based upgrades, DR relies heavily on user participation, which introduces behavioral variability into grid operations. This variability, however, is not a weakness but a strategic advantage when properly managed. It allows the grid to function more like an intelligent ecosystem, capable of self-regulation through distributed decision-making. The integration challenge thus becomes one of harmonizing consumer flexibility with system-wide optimization—an undertaking that reflects both the adaptive ambitions of pragmatism and the protective imperatives of securitism. Furthermore, DR integration is particularly relevant for managing the growing complexity of electricity systems, especially those incorporating large shares of renewable energy. Wind and solar power, though sustainable, introduce intermittency into the grid. DR provides a flexible counterbalance to this variability by adjusting consumption to match fluctuating supply. This ensures that the grid remains both balanced and efficient, even in the face of unpredictable energy inputs. As Alizdeh *et al*. (2016) argue, the strategic incorporation of DR enhances not only cost savings but also system resilience, thereby contributing to long-term sustainability and grid modernization.

Building upon the foundational theoretical framework, we construct the reasoning that underpins the development of the second hypothesis as follows:

H2: Demand Response Integration has a positive impact on Smart Grid Operational Efficiency.

2.5 Moderating Role of Cybersecurity Readiness

Cybersecurity readiness refers to the preparedness of digital infrastructure and institutional systems to identify, prevent, respond to, and recover from cyber threats that could compromise technological integrity and operational continuity (Wang *et al.,* 2024). Within the context of smart grid modernization, cybersecurity readiness includes technical capabilities—such as intrusion detection, encryption, and network resilience—as well as strategic components like risk governance, staff training, and incident response protocols (Gunduz & Das, 2020). This concept is especially critical in high-automation environments such as smart grids, where core functions rely on uninterrupted data flows and real-time analytics powered by artificial intelligence.

In this study, cybersecurity readiness acts as a moderating variable that conditions the effectiveness of AI-based predictive maintenance in enhancing smart grid operational efficiency. Predictive maintenance systems rely on large volumes of data collected from smart meters, IoT sensors, and industrial control systems to detect anomalies and forecast potential equipment failures. Without sufficient cybersecurity measures, this data can be intercepted, manipulated, or rendered inaccessible, thereby undermining the reliability of AI-based predictions (Khurana *et al.,* 2010). When cybersecurity systems are robust, predictive maintenance tools are able to function accurately, scheduling timely interventions that reduce outages and optimize asset life cycles. This secured operational environment ensures that the AI's predictive power translates directly into improved grid performance, minimized energy loss, and cost savings. In contrast, in low-readiness environments, cyber vulnerabilities expose AI tools to disruptions such as false data injection or denial-of-service attacks, significantly weakening their impact on operational outcomes.

The moderating role of cybersecurity readiness in this project reflects a growing recognition that digital transformation alone is not sufficient for optimizing infrastructure performance. As Christopher *et al.* (2014) emphasize, cybersecurity must be structurally embedded within digital systems, particularly when AI tools are entrusted with high-stakes operational functions. The characteristic complexity of this moderating relationship lies in its systemic nature: cybersecurity is not a standalone input but a foundational condition that shapes the consistency, accuracy, and resilience of AI-enabled grid innovations (Alsuwian *et al.,* 2022) Ultimately, cybersecurity readiness transforms AI from a theoretical asset into a reliable operational tool—thus reinforcing smart grid efficiency and sustaining the trust necessary for further digital advancement.

Based on the guiding theoretical framework and perspectives, the reasoning for hypothesis three is articulated below:

H3: Cybersecurity readiness moderates the impact of AI-based predictive maintenance on smart grid operational efficiency.

Grounded in robust theoretical foundations, this study enhances its academic significance through the presentation of the following conceptual framework.

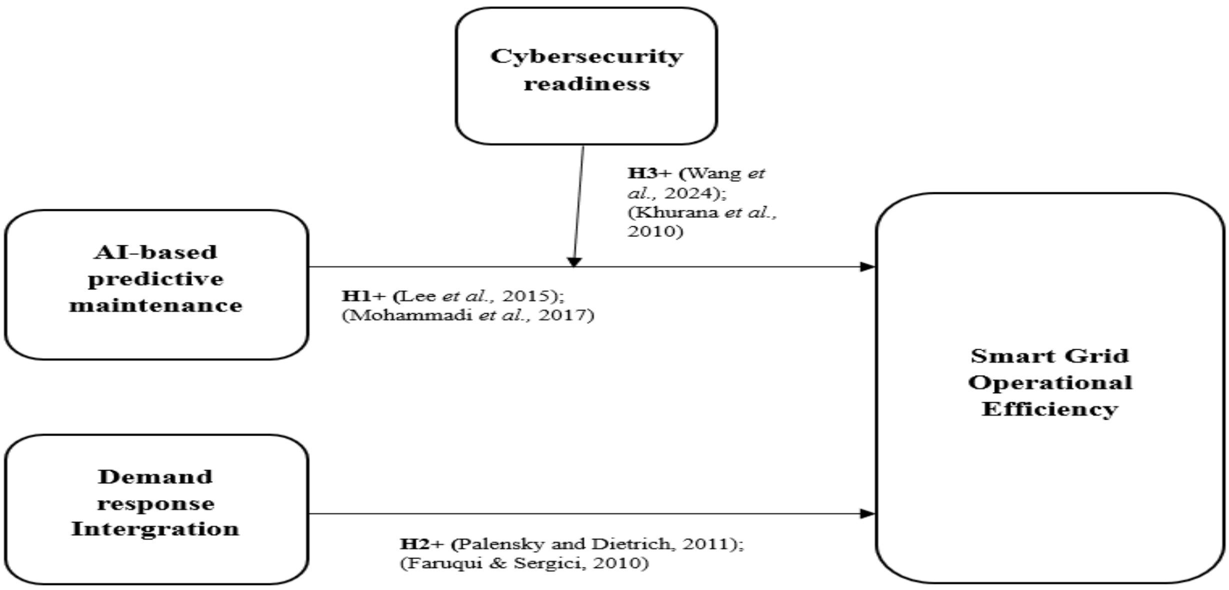

Figure 1: The Paper Conceptual Framework

3. METHODS

3.1 Research approach and strategy

This study utilized a quantitative research approach, which enables the systematic collection and interpretation of numerical data to detect and validate patterns (Creswell & Creswell, 2017). Statistical techniques were applied to objectively analyze the data and generate measurable outcomes (Babbie, 2010). This methodology was selected to align with the research objectives and explore the connections among key variables. Additionally, a deductive reasoning framework was employed—well-suited to quantitative research—as it supports hypothesis testing, predictive insights, and evidence-based conclusions derived from statistical findings.

3.2 Participants

This study used a purposive stratified sample technique to target experts involved in the development, operation, or cybersecurity management of smart grid systems in Vietnam in order to guarantee empirical robustness and sectoral relevance. Participants had to have at least two years of real-world experience in positions involving energy infrastructure management, smart grid operations, or digital security in critical infrastructure in order to be eligible. Four major professional and functional categories were stratified in order to guarantee contextual depth and representational diversity:

1. In utility firms, AI-based predictive maintenance solutions are deployed or managed by grid operations engineers and maintenance specialists. These people support preventative maintenance plans, anomaly detection, and real-time system monitoring;
2. Energy systems analysts and smart grid designers engaged in demand response solution planning, modeling, or integration, digital control systems, and energy distribution optimization;
3. Digital infrastructure managers and cybersecurity officers, who are responsible for monitoring threat detection, putting security policies into place, and guaranteeing data integrity across IoT-enabled networks and energy management systems;
4. Policy advisors, regulators, and consultants for the energy sector who help create cybersecurity frameworks, grid modernization regulations, and national or regional digital transformation programs.

Eligible participants had to have direct experience with at least one of the following: designing demand response programs, deploying AI-based maintenance, or conducting cybersecurity preparedness assessments for energy infrastructure. Professional function, organizational role, technical specialty, and exposure to smart grid innovation initiatives were among the stratification factors. Professional networks including Vietnam Electricity (EVN) technical divisions and the Vietnam Smart Grid Community were used to distribute the survey, which was distributed using secure online channels like Google Forms and institutional mailing lists. Cybersecurity symposia in Southeast Asia, digital transformation seminars, and LinkedIn energy forums were used for additional outreach.

A 5-point Likert scale, with 1 denoting "strongly disagree" and 5 denoting "strongly agree," was used in the survey instrument to gauge respondents' opinions on the usefulness of AI-based predictive maintenance, the function of demand response in grid optimization, and the moderating effect of cybersecurity readiness. After being screened for completeness, relevance, and internal consistency, 385 legitimate replies were kept out of the 743 responses that were gathered. A thorough quantitative investigation of the ways in which cybersecurity readiness and developing technologies affect operational efficiency in digitalized energy systems was made possible by the stratified and varied respondent population.

4. RESULTS

4.1. Reliability analysis

Table 1: Reliability analysis of "smart grid operational efficiency". Source: (The authors, 2025)

Reliability Statistics

Cronbach's Alpha	N of Items
.635	4

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
SG1	7.913	7.112	.602	.628
SG2	7.051	7.220	.569	.617
SG3	7.614	7.412	.569	.584

SG4	8.587	8.938	.573	.588

Where the survey items SG1 through SG4 correspond to questions 1 to 4 measuring the construct of smart grid operational efficiency (SG).

As shown in Table 1, each of these dependent sub-variables yielded adjusted item-total correlation values of at least 0.3. The overall Cronbach's alpha coefficient was 0.635, exceeding the commonly accepted threshold of 0.6 and outperforming any alternative values that would have resulted from removing individual items. Additionally, all sub-items demonstrated Cronbach's alpha values higher than their respective adjusted item-total correlations, even when considered in isolation. Therefore, all four items were deemed reliable and retained for further analysis. A similar level of internal consistency was also observed in the Cronbach's alpha results for the remaining variables.

4.2. Exploratory factor analysis (EFA)

Table 2: Rotated Component Matrix. Source: (The authors, 2025)

Rotated Component Matrix[a]			
Component with loading factors			
1	2	3	4
SG1 .633	AP1 .570	DI1 .515	CR1 .630
SG2 .577	AP2 .580	DI2 .508	CR2 .585
SG3 .546	AP3 .606	DI3 .612	CR3 .672
SG4 .647	AP4 .676	DI4 .682	CR4 .645
Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.			
a. Rotation converged in 7 iterations.			

Where survey items AP1 to AP4, DI1 to DII4, and CR1 to CR4 were developed to assess two independent variables and the moderator, respectively, through questions 1 to 4 of each construct. As reported in Table 2, the rotated component matrix effectively grouped the 16 sub-items into four distinct factors, corresponding precisely to the dependent variable, the two independent variables, and the moderator variable. All items exhibited factor loadings above the 0.5 threshold, confirming their relevance to the intended constructs. Consequently, no items were excluded during the factor analysis, indicating strong construct validity across all variables.

4.3. Multiple linear regression model

Table 3: Coefficients[a]. Source: (The authors, 2025)

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	6.652	.709		4.361	.000
	AP	.648	.865	.635	3.727	.008
	DI	.520	.732	.508	3.477	.027

a. Dependent Variable: SG

Where **SG**: mean of SG1 to SG4; **AP**: mean of AP1 to AP4; **DI**: mean of DI1 to DI4

As illustrated in Table 3, the t-test results yielded significance (Sig.) values of .008 and .027, both falling below the standard alpha level of 0.05. This indicates that the independent variables, AI-based predictive maintenance and demand response integration, have a statistically significant influence on the dependent variable, smart grid operational efficiency. Accordingly, the findings provide empirical support for both proposed hypotheses.

4.4. Moderator analysis

Table 4: Results analysis of "cybersecurity readiness". Source: (The authors, 2025)

Model : 1
Y : SG
X : AP
W : CR
Sample Size: 385
****

OUTCOME VARIABLE:
SG
Model Summary

R	R-sq	MSE	F	dl1	dl2	p
.638	.619	.730	5.666	3.000	381.000	.000

Model

	coeff	se	t	p	LLCI	ULCI
constant	7.272	.615	61.361	.000	7.848	7.583
AP	.639	.621	4.822	.000	.765	.751
CR	.545	.734	4.317	.000	.605	.598
Int_1	.472	.902	4.566	.000	.603	.589

Where **CR**: mean of CR1 to CR4

As presented in Table 4, the p-value associated with the interaction term (Int_1) is 0.000, well below the conventional significance threshold of 0.05. This signifies a statistically significant interaction effect between AI-based predictive maintenance and cybersecurity readiness on smart grid operational efficiency. The interaction coefficient of 0.472 suggests that stronger cybersecurity readiness amplify the positive influence of AI-based predictive maintenance on smart grid operational efficiency. As a result, hypothesis H3 is empirically supported.

5. DISCUSSION

5.1. Result Summary

Demand response integration and AI-based predictive maintenance have respective coefficients of 0.508 and 0.635 on smart grid operational efficiency. Additionally, with a coefficient of 0.472, cybersecurity readiness moderates the impact of AI-based predictive maintenance on smart grid operational efficiency.

5.2. Theoretical Implications

The instrumentalist belief that technology instruments are useful only when they provide quantifiable operational results is supported by the notable improvement in smart grid operational efficiency ($\beta = 0.635$) that AI-based predictive maintenance brings (Heidegger, 1977). The results are quite consistent with the claims made by Lee *et al*. (2015) and Mohammadi *et al.* (2017) that AI-powered diagnostics significantly lower outages and increase asset longevity. Our findings highlight that predictive maintenance's performance is entwined with worker preparedness and larger digital infrastructures, as Büscher and Sumpf (2015) pointed out. This article, however, deviates from the optimistic assumptions of Zhou *et al.* (2016), who consider predictive maintenance to be self-sufficient. Our data only partially supports the technologism school's claim that efficiency is driven only by innovation (Feenberg, 2012); the influence of AI is contingent upon an organization's capacity to comprehend and respond to algorithmic projections. Therefore, this study highlights the necessity of integrative systems thinking in smart grid modernization by criticizing deterministic framings of AI in favor of socio-technical interdependence, as highlighted by Trist (1981).

Faruqui and Sergici's (2010) claim that demand response integration (DR) lowers peak demand and enhances grid responsiveness is supported by empirical evidence of its impact on smart grid operational efficiency ($\beta = 0.508$). This analysis supports Palensky and Dietrich's (2011) conceptualization of DR as a decentralized, digitally mediated load balancing mechanism. But by exposing that DR's effects depend on socio-behavioral coordination, it challenges their techno-optimism and echoes Gyamfi et al. (2013)'s worries about user unpredictability. The results demonstrate that behavioral variability, when appropriately integrated, functions as a dynamic advantage rather than an operational danger, which runs counter to Siano's (2014) strict efficiency rationale. Dewey's (1929) use of pragmatism is upheld, establishing DR as an adaptive system motivated by response to the real world rather than a prescriptive paradigm. Furthermore, the study casts doubt on the notion that disaster recovery systems are intrinsically safe; as

Liu et al. (2024) warn, cyberattacks erode confidence in these systems. Therefore, this study supports a hybrid approach in which efficiency is a combination of behavioral flexibility and technology design.

According to Khurana et al. (2010) and Alsuwian et al. (2022), predictive systems turn into liabilities rather than advantages in the absence of secure digital channels and intrusion resistance. This viewpoint contradicts Lee et al. (2015)'s deterministic position, which downplays the infrastructure vulnerability of AI technologies in grid settings. The analysis provides significant support for Christopher et al. (2014)'s systems-based theory, which holds that cybersecurity is a fundamental facilitator of technical success rather than an ancillary issue. This study challenges the linearity of Feenberg's (2012) technology, which sees innovation as a natural progression, by showing how unprotected AI implementations run the danger of escalating system vulnerabilities. We contend, using Trist (1981), that grid efficiency depends on the incorporation of AI into cyber-resilient organizational structures rather than AI in and of itself. In order to reframe predictive maintenance as being only successful when integrated into strong digital governance structures, the article presents a securitized socio-technical paradigm.

5.3. Practical Implications

The results have important ramifications for utility operators, cybersecurity strategists, and energy regulators. First, utility companies should invest in machine learning-based diagnostics to decrease downtime and increase asset longevity, since AI-based predictive maintenance has a significant impact on smart grid efficiency (Mohammadi et al., 2017). Büscher and Sumpf (2015) stress that in order to achieve successful organizational acceptance, this implementation must be complemented with human-centered training and process improvement. Second, grid operators should improve real-time responsiveness through automated control systems and dynamic pricing mechanisms, which have been demonstrated to reduce peak load by up to 20%. This is because demand response integration has a significant impact on operational efficiency (Albadi & El-Saadany, 2008). According to Gyamfi et al. (2013), consumer involvement is still difficult to achieve, thus behaviorally informed incentive schemes must be jointly created to guarantee continued participation. Third, the viability of AI systems depends on cybersecurity preparedness, which is more than just a technological precaution. Predictive algorithms are vulnerable to control hijacking and data poisoning due to insecure infrastructures (Khurana et al., 2010). Therefore, in order to systematically audit, update, and control digital defenses, national energy policies should embrace cybersecurity capability maturity models (Christopher et al., 2014). In practice, this entails incorporating cybersecurity awareness at every level of the company and integrating multi-layered security, from centralized risk governance to encrypted IoT endpoints. All of these results support a concerted socio-technical change in grid modernization that strikes a balance between security, resilience, and creativity.

5.4. Limitations

This study has limitations in spite of its contributions. First, the study is primarily focused on Vietnam, which would restrict the findings' applicability to energy markets that are more developed or less digitalized. Second, causal inference is limited since the cross-sectional design records perceptions at a single moment in time. Third, answer bias may be introduced by the use of self-reported data, especially when it comes to cybersecurity capacity questions. Last but not least, even though the constructs were theoretically based, future research might incorporate other mediators or organizational elements—like regulatory support or automation trust—to capture more intricate dynamics in smart grid performance.

5.5. Future Research Directions

In order to examine how institutional maturity influences the link between new technologies and grid efficiency, future research should expand this concept across other geopolitical situations. To document how AI and demand response systems have changed over time, especially in light of growing cyberthreats and stresses brought on by the climate, longitudinal studies are required. Furthermore, in order to more accurately forecast consumer reaction to demand-side actions, future models have to incorporate behavioral economics and digital literacy characteristics. Investigating multi-actor partnerships, such as public-private partnerships, may also provide information on how dispersed governance frameworks influence energy innovation and cybersecurity preparedness at the same time.

5.6. Conclusion

This paper provides a thorough analysis of the ways in which demand response integration and AI-based predictive maintenance affect smart grid operational efficiency, with cybersecurity preparedness acting as a moderator. It illustrates that institutional preparedness and digital resilience are essential; technology solutions cannot provide value in isolation, drawing on socio-technical systems and contingency theory. The empirical findings support all three theories and provide useful information for energy modernization as well as theoretical enrichment. In the end, the results highlight the fact that smart grid effectiveness depends on more than just technological advancement; in an increasingly unstable digital energy market, it necessitates synchronized alignment of data security, organizational capabilities, and adaptable infrastructure.

REFERENCES

1) Albadi, M. H., & El-Saadany, E. F. (2008). A summary of demand response in electricity markets. *Electric power systems research*, *78*(11), 1989-1996. https://doi.org/10.1016/j.epsr.2008.04.002
2) Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International journal of critical infrastructure protection*, *8*, 53-66.https://doi.org/10.1016/j.ijcip.2014.12.002
3) Alizadeh, M. I., Moghaddam, M. P., Amjady, N., Siano, P., & Sheikh-El-Eslami, M. K. (2016). Flexibility in future power systems with high renewable penetration: A review. *Renewable and Sustainable Energy Reviews*, *57*, 1186-1193. https://doi.org/10.1016/j.rser.2015.12.200
4) Almeida, M., Ascione, F., Iaccheo, A., Iovane, T., & Mastellone, M. (2025). Towards the Necessary Decarbonization of Historic Buildings: A Review. *Energies*, *18*(3), 502. https://doi.org/10.3390/en18030502
5) Alsuwian, T., Shahid Butt, A., & Amin, A. A. (2022). Smart grid cyber security enhancement: Challenges and solutions—A review. *Sustainability*, *14*(21), 14226. https://doi.org/10.3390/su142114226
6) Büscher, C., & Sumpf, P. (2015). “Trust” and “confidence” as socio-technical problems in the transformation of energy systems. *Energy, sustainability and Society*, *5*, 1-13.
7) Cherns, A. (1987). Principles of sociotechnical design revisted. *Human relations*, *40*(3), 153-161.
8) Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., & Dolan, T. (2014). Cybersecurity capability maturity model (C2M2). *Department of Homeland Security*, 1-76.
9) Dewey, J. (1929). *The quest for certainty: A study of the relation of knowledge and action* (Vol. 28). Putnam Adult.
10) Donaldson, L. (2001). *The contingency theory of organizations*. Sage. https://doi.org/10.4135/9781452229249
11) Fang, X., Misra, S., Xue, G., & Yang, D. (2011). Smart grid—The new and improved power grid: A survey. *IEEE communications surveys & tutorials*, *14*(4), 944-980. https://doi.org/10.1109/SURV.2011.101911.00087
12) Faruqui, A., & Sergici, S. (2010). Household response to dynamic pricing of electricity: a survey of 15 experiments. *Journal of regulatory Economics*, *38*(2), 193-225. https://doi.org/10.1007/s11149-010-9127-y
13) Fatima, S., & Arshad, M. J. (2025). A Comprehensive Review of Blockchain and Machine Learning Integration for Peer-to-Peer Energy Trading in Smart Grids. *IEEE Access*.
14) Feenberg, A. (2012). *Questioning technology*. routledge.
15) Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094
16) Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. *IEEE transactions on Industrial informatics*, *7*(4), 529-539. https://doi.org/10.1109/TII.2011.2166794
17) Gyamfi, S., Krumdieck, S., & Urmee, T. (2013). Residential peak electricity demand response—Highlights of some behavioural issues. *Renewable and Sustainable Energy Reviews*, *25*, 71-77. https://doi.org/10.1016/j.rser.2013.04.006
18) Hasegawa, K., O'Brien, N., Prendergast, M., Ajah, C. A., Neves, A. L., & Ghafur, S. (2024). Cybersecurity Interventions in Health Care Organizations in Low-and Middle-Income Countries: Scoping Review. *Journal of medical Internet research*, *26*, e47311. https://doi.org/10.2196/47311
19) Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of “big data” on cloud computing: Review and open research issues. *Information systems*, *47*, 98-115. https://doi.org/10.1016/j.is.2014.07.006
20) Heidegger, M. (1977). The question concerning technology. *New York*, *214*, 2013.
21) Khan, A. A., Rehmani, M. H., & Reisslein, M. (2015). Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols. *IEEE Communications Surveys & Tutorials*, *18*(1), 860-898. https://doi.org/10.1109/COMST.2015.2481722
22) Khurana, H., Hadley, M., Lu, N., & Frincke, D. A. (2010). Smart-grid security issues. *IEEE Security & Privacy*, *8*(1), 81-85. https://doi.org/10.1109/MSP.2010.49
23) Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, *3*, 18-23. https://doi.org/10.1016/j.mfglet.2014.12.001

24) Li, F., Luo, B., & Liu, P. (2010, October). Secure information aggregation for smart grids using homomorphic encryption. In *2010 first IEEE international conference on smart grid communications* (pp. 327-332). IEEE. https://doi.org/10.1109/SMARTGRID.2010.5622064
25) Liu, M., Teng, F., Zhang, Z., Ge, P., Sun, M., Deng, R., ... & Chen, J. (2024). Enhancing cyber-resiliency of der-based smart grid: A survey. *IEEE Transactions on Smart Grid*. https://doi.org/10.1109/TSG.2024.3373008
26) Luthra, S., Janssen, M., Rana, N. P., Yadav, G., & Dwivedi, Y. K. (2023). Categorizing and relating implementation challenges for realizing blockchain applications in government. *Information Technology & People*, *36*(4), 1580-1602. https://doi.org/10.1108/ITP-08-2020-0600
27) Mohammadi, M., Al-Fuqaha, A., Guizani, M., & Oh, J. S. (2017). Semisupervised deep reinforcement learning in support of IoT and smart city services. *IEEE Internet of Things Journal*, *5*(2), 624-635. https://doi.org/10.1109/JIOT.2017.2712560
28) Palensky, P., & Dietrich, D. (2011). Demand side management: Demand response, intelligent energy systems, and smart loads. *IEEE transactions on industrial informatics*, *7*(3), 381-388. https://doi.org/10.1109/TII.2011.2158841
29) Safari, A., Daneshvar, M., & Anvari-Moghaddam, A. (2024). Energy Intelligence: A Systematic Review of Artificial Intelligence for Energy Management. *Applied Sciences*, *14*(23), 11112. https://doi.org/10.3390/app142311112
30) Siano, P. (2014). Demand response and smart grids—A survey. *Renewable and sustainable energy reviews*, *30*, 461-478. https://doi.org/10.1016/j.rser.2013.10.022
31) Trist, E. L. (1981). *The evolution of socio-technical systems* (Vol. 2, p. 1981). Toronto: Ontario Quality of Working Life Centre.
32) Wang, C., Bi, Z., & Da Xu, L. (2014). IoT and cloud computing in automation of assembly modeling systems. *IEEE Transactions on Industrial Informatics*, *10*(2), 1426-1434. https://doi.org/10.1109/TII.2014.2300346
33) Wang, X., Li, S., & Rahman, M. A. (2024). A comprehensive survey on enabling techniques in secure and resilient smart grids. *Electronics*, *13*(11), 2177. https://doi.org/10.3390/electronics13112177
34) Yin, S., & Kaynak, O. (2015). Big data for modern industry: challenges and trends [point of view]. *Proceedings of the IEEE*, *103*(2), 143-146. https://doi.org/10.1109/JPROC.2015.2388958
35) Zhou, K., Fu, C., & Yang, S. (2016). Big data driven smart energy management: From big data to big insights. *Renewable and sustainable energy reviews*, *56*, 215-225. https://doi.org/10.1016/j.rser.2015.11.050
36) Babbie, E. (2010). The practice of social research (12th ed.). Wadsworth.
37) Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

APPENDIX: Survey

Table 6. Survey Questionnaire

Background information

What is your primary professional role in relation to smart grid systems?	Grid Operations / Maintenance Engineer	Energy Systems Analyst / Smart Grid Planner	Cybersecurity Officer / Digital Infrastructure Manager	Policy Advisor / Energy Sector Consultant	Other (Please specify): ___________	
How many years of experience do you have working with smart grid technologies, energy infrastructure, or cybersecurity systems?	Less than 2 years	2–5 years	6–10 years	More than 10 years		

Which of the following smart grid activities have you directly participated in? *(Select all that apply)*	Designing or implementing demand response programs	Deploying AI-based predictive maintenance systems	Conducting cybersecurity assessments for energy infrastructure	Developing smart grid regulations or digital policies	Other (please specify): ___________	
What type of organization do you currently work for?	State-owned utility company (e.g., EVN)	Private energy or technology firm	Government/regulatory agency	Academic or research institution	International organization or consulting firm	Other (please specify): ____________

o.	**Variables**	**Coded Sub-variables**	**Content**
1.	Smart Grid Operational Efficiency	SG1	The use of smart grid technologies reduces system downtimes and enhances service reliability (Fatima & Arshad, 2025).
		SG2	Real-time monitoring and data-driven decisions help optimize energy flow in smart grids (Fang et al., 2011).
		SG3	Smart grid systems minimize transmission losses and extend asset lifespan (Siano, 2014).
		SG4	Institutional coordination and cybersecurity readiness are essential for achieving grid efficiency (Güngör et al., 2011).
2.	AI-Based Predictive Maintenance	AP1	AI-based maintenance systems reduce unexpected equipment failures (Lee et al., 2015).
		AP2	Predictive analytics extend the lifespan of grid assets (Mohammadi et al., 2017).
		AP3	AI tools allow for real-time detection of system anomalies (Wang et al., 2014).
		AP4	The effectiveness of predictive maintenance depends on data quality and operator readiness (Büscher & Sumpf, 2015).
3.	Demand Response Integration	DI1	Demand response mechanisms help reduce peak load and balance energy supply (Faruqui & Sergici, 2010).
		DI2	Automated DR systems improve economic efficiency and operational responsiveness (Safari et al., 2024).
		DI3	DR strategies require active consumer participation and behavioral coordination (Gyamfi et al., 2013).
		DI4	Cybersecurity threats can impact the reliability of DR programs (Liu et al., 2024).
4.	Cybersecurity Readiness	CR1	Our systems have strong intrusion detection and data protection protocols in place (Gunduz & Das, 2020).
		CR2	Cybersecurity policies and training are embedded across the organization (Christopher et al., 2014).

		CR3	We regularly audit and update our cybersecurity infrastructure to meet evolving threats (Alsuwian et al., 2022).
		CR4	Cybersecurity readiness enables AI tools to function accurately and securely (Khurana et al., 2010).

Survey link: https://forms.gle/Sz58LFDSrRGaxbyA8