ISSN: 2633-4828 Vol. 5 No.S2, (Mar – Apr 2023)

International Journal of Applied Engineering & Technology

OPERATIONAL RESILIENCE BY DESIGN: A CONTINUITY ASSURANCE MODEL FOR MODERNIZING CRITICAL ENERGY APPLICATIONS

Jagadeesh Vedula
IT Project Manager (Digital Transformation), Meghaz Inc.
jagadeeshvedula79@gmail.com

ABSTRACT

Modernizing the critical functions of the oil and gas industry, from upstream exploration and production through midstream pipeline transport and downstream refining and distribution, depends increasingly on digital technologies, cloud-native platforms, the industrial internet of things (IIoT), and artificial intelligence (AI) embedded within process control and pipeline monitoring systems. These advancements have improved operational efficiency and scalability, but they have also introduced new risks for critical energy applications, including cyber-attacks on SCADA and industrial control systems, equipment failures, supply chain disruptions, and extreme weather events. This paper proposes a continuity assurance model, Operational Resilience by Design (ORD), that applies resilience principles across the full lifecycle of critical oil and gas applications rather than treating continuity as a reactive, post-incident process. The proposed framework incorporates resilient architecture, zero trust security, predictive monitoring, automatic fail-over, and disaster recovery, along with digital twins and continuous validation, to help ensure that pipeline, refinery, and field operations remain available under adverse conditions. In relation to business continuity, regulatory compliance, and the reduction of recovery time objective (RTO) and recovery point objective (RPO), the proposed model provides assurance of operational resilience for critical oil and gas applications. A layered framework is proposed to support improved reliability, real-time situational awareness, fault tolerance, and adaptive decision-making across distributed upstream, midstream, and downstream infrastructure. The layered framework also supports modernization initiatives by enabling secure migration from legacy operational technology (OT) systems to cloud-enabled platforms while preserving system availability. Findings indicate that embedding resilience into system design improves system reliability, operational continuity, and preparedness for cyber threats. The proposed continuity assurance model offers oil and gas operators a practical roadmap for developing secure, adaptive, and sustainable critical infrastructure capable of withstanding the evolving nature of operational and cyber threats.

Keywords— Operational Resilience by Design (ORD), Cyber Resilience, Zero Trust Architecture, Digital Twins, Industrial Internet of Things.

I. INTRODUCTION

The global oil and gas industry is undergoing a significant digital transformation driven by cloud-based technologies, the Industrial Internet of Things (IIoT), AI, edge computing, and advanced analytics. Critical oil and gas applications, including upstream exploration and production, midstream pipeline transportation and storage, and downstream refining and distribution, increasingly rely on interconnected digital platforms to improve operational efficiency, support predictive maintenance programs, and enable timely, data-driven decision-making. **[1]**.

The digitalization of oil and gas operations has increased performance and scalability, but it has also expanded the cyberattack surface and the overall complexity of operations. Critical infrastructure such as pipelines, refineries, and offshore platforms is exposed to an increasingly sophisticated range of cyber threats, together with risks from software vulnerabilities, hardware failures, supply chain attacks, communication outages, and severe weather events, any of which could disrupt hydrocarbon supply and threaten economic stability. As a result, continuous operation has become a key strategic objective for oil and gas operators, regulators, and the broader critical infrastructure community.

Traditional approaches to disaster recovery and Business continuity are largely centered around restoring services post disruption. Today's oil and gas infrastructures need proactively resilient systems that preemptively anticipate, absorb, recover from, and adapt to unexpected cyber and operational incidents [3]. As a result, operational resilience has developed into an all-encompassing discipline that integrates cyber security, operational reliability engineering, business continuity, risk management and governance into one operational framework.

The convergence of Information Technology (IT), Operational Technology (OT), SCADA systems, cloud-native platforms, and remote field instrumentation has transformed conventional pipeline, refinery, and production systems into tightly linked cyber-physical infrastructures [4]. While this convergence enables smart automation and more efficient asset management, it also introduces new vulnerabilities that require resilient architectures capable of maintaining connectivity and delivering essential services under difficult operating conditions.

As an engineering philosophy, Operational Resilience by Design (ORD) is a proactive method of embedding resilience into the lifecycle of a critical energy application. Instead of considering resilience as a capability after deployment, the proposed approach incorporates fault-tolerant architectures, Zero Trust Security, predictive monitoring, automated failovers, orchestration of disaster recovery, digital twins and continuous validation into the design process of the system [5] to improve service availability while reducing Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).

Additionally, regulatory agencies and international standards increasingly require oil and gas operators to demonstrate operational continuity, cyber resiliency, incident-response preparedness, and supply chain security as core components of their digital modernization initiatives [6]. Meeting these evolving requirements calls for resilient-by-design applications capable of sustaining critical operations during significant cyber or physical disruptions. This study presents a Continuity Assurance Model built on the principles of Operational Resilience by Design for the modernization of critical oil and gas applications. The model incorporates resilient system architecture, intelligent monitoring, adaptive governance, automated recovery mechanisms, and continuous assurance practices to improve reliability, cybersecurity, operational continuity, and sustainable modernization of critical energy infrastructure.

II. LITERATURE REVIEW

Modernization of critical oil and gas operations is accelerating due to growing adoption of cloud computing, the Industrial Internet of Things (IIoT), artificial intelligence (AI), edge computing, and software-defined infrastructure (SDI). These technologies improve operational efficiency and support digital oilfield and pipeline network management, but they also increase system complexity and expand the attack surface for cyber-attacks on critical infrastructure. This underscores the need for continued research into the operational reliability of oil and gas systems as they evolve toward more secure and resilient architectures **[7]**.

Much of the foundational literature on resilience engineering originates in the electric power sector, but the underlying principles translate directly to oil and gas cyber-physical systems, since both domains rely on SCADA, industrial control systems (ICS), and increasingly converged IT/OT environments. Early research on the evolution of conventional utility infrastructure into sophisticated, connected systems highlighted a growing requirement for enhanced communications, automated technologies, and robust cybersecurity methods to support reliable service delivery amid increasing system complexity, establishing a framework for resilient cyber-physical architectures [8]. Building on this work, subsequent research surveyed cybersecurity issues affecting cyber-physical systems more broadly, including vulnerabilities within Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and the Industrial Internet of Things (IIoT) — vulnerabilities that are equally present in oil and gas pipeline and refinery control environments. That work concluded that sustaining continuous operations during a cyber-intrusion requires design approaches that integrate both resilient system architecture and protected communications.

A growing number of cyberattacks targeting energy infrastructure highlights the need for resilience engineering across the sector. The 2021 ransomware attack on the Colonial Pipeline system in the United States demonstrated

how a single intrusion into IT infrastructure could force the shutdown of a major fuel pipeline, disrupting downstream fuel supply across multiple states even though the operational technology (OT) environment itself was not directly compromised [2]. Findings from investigations into this and comparable incidents highlighted the shortcomings of relying solely on perimeter-based security and emphasized the need for continuous monitoring, rapid incident response, and resilient operational architectures purpose-built for pipeline and process control environments. Resiliency has since been studied as a multidimensional capability encompassing robustness, adaptability, recoverability, and operational flexibility. Related research proposed a conceptual model that differentiates resiliency from standard reliability by focusing on how well an operator can withstand and recover from low-probability, high-consequence events, integrating infrastructure hardening, operational flexibility, and adaptive control mechanisms. Quantitative methodologies were also developed to assess resiliency by combining infrastructure reinforcement with intelligent operational enhancement strategies. This body of research concludes that integrating predictive analytics, distributed monitoring, and adaptive restoration methodologies can substantially improve the ability of critical infrastructure systems to withstand disruption and minimize service interruption **[9]**.

An alternate view of resilience supports measurable resilience metrics drawn from diverse areas of critical infrastructure systems. This work provides a framework based on anticipation, absorption, recovery, and adaptation as four key characteristics that need to be integrated into governance and decision-making for infrastructure systems, suggesting that resilience should be continuously evaluated using performance indicators rather than measured only as a final reliability outcome. Related research has worked toward standardized resilience taxonomies for critical infrastructure, reviewing the literature on different definitions of power system resilience and developing a holistic taxonomy that integrates four categories: physical infrastructure, cyber resilience, operational preparedness, and recovery capability. Although this taxonomy was developed for electric power systems, the same categories map directly onto oil and gas infrastructure, where physical asset integrity, cyber resilience of SCADA and ICS environments, operational preparedness, and recovery capability are equally central concerns, making this taxonomy a useful foundation for resilience-by-design methodologies in today's oil and gas applications. Substantial progress has been made on power-sector resilience; however, the bulk of existing research on critical energy infrastructure focuses on cybersecurity, infrastructure hardening, or disaster recovery as their own distinct silos. Little research has gone into incorporating all aspects of resilience into every stage of the application lifecycle for oil and gas systems specifically, such as software architecture, cloud migration, continuous validation, automated failover, governance, and business continuity assurance.

In addition, a number of current frameworks do not offer an integrated solution for achieving operational resilience alongside cybersecurity and digital modernization within the same critical oil and gas environment. To address this shortcoming, the purpose of this research is to present the Operational Resilience by Design (ORD) Continuity Assurance Model, which integrates resilience principles throughout the architecture, development, deployment, monitoring, and management of critical oil and gas software and applications. A key outcome of this proposed framework is that it creates a bridge between traditional business continuity planning and the next generation of resiliency engineering by combining fault-tolerant architecture, Zero Trust Security models, digital twins, predictive monitoring, automatic recovery, and continuous validation as part of an overall modernization strategy [10], [11].

Stakeholder Perspectives on Oil and Gas System Resilience

Although there are many technical definitions of resilience in critical energy systems, this paper also takes a stakeholder-centric view and asks whether an oil and gas system that strictly follows these definitions can genuinely serve the needs of operators, regulators, downstream fuel consumers, and communities near pipeline and refining assets. Here we look at how service reliability, supply continuity, and safety impact stakeholder views on the resilience of oil and gas systems. The next subsections go into additional detail on how these characteristics shape stakeholder perceptions of resilience, as seen in Fig. 2.

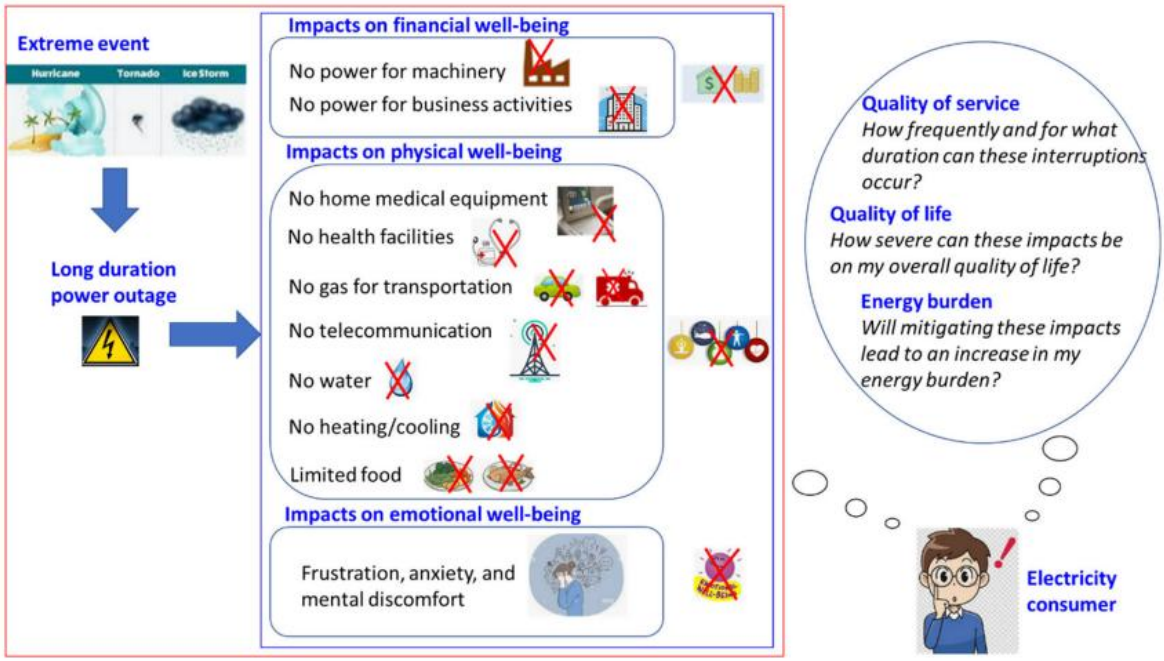

Figure 2. Example of how stakeholders perceive resilience in oil and gas operations.

III. RESEARCH FRAMEWORK

The Operational Resiliency by Design (ORD) framework provides a systematic approach to modernizing and improving the resilience of critical oil and gas applications so that they can continue delivering services through cyber, operational, or environmental disruptions. The ORD framework provides a Continuity Assurance Model (CAM) that integrates the disciplines of resilience engineering, cybersecurity, cloud-native modernization, business continuity, and intelligent monitoring into one cohesive system. Unlike traditional post-incident recovery methods, the framework builds resiliency into an application across its entire lifecycle, allowing the systems that support pipeline, refinery, and field operations to proactively prepare for, withstand, recover from, and adapt to emerging threats [12]. The research framework comprises six layers, vertically and horizontally connected, that work together to strengthen operational resiliency across the oil and gas sector and its associated critical infrastructure.

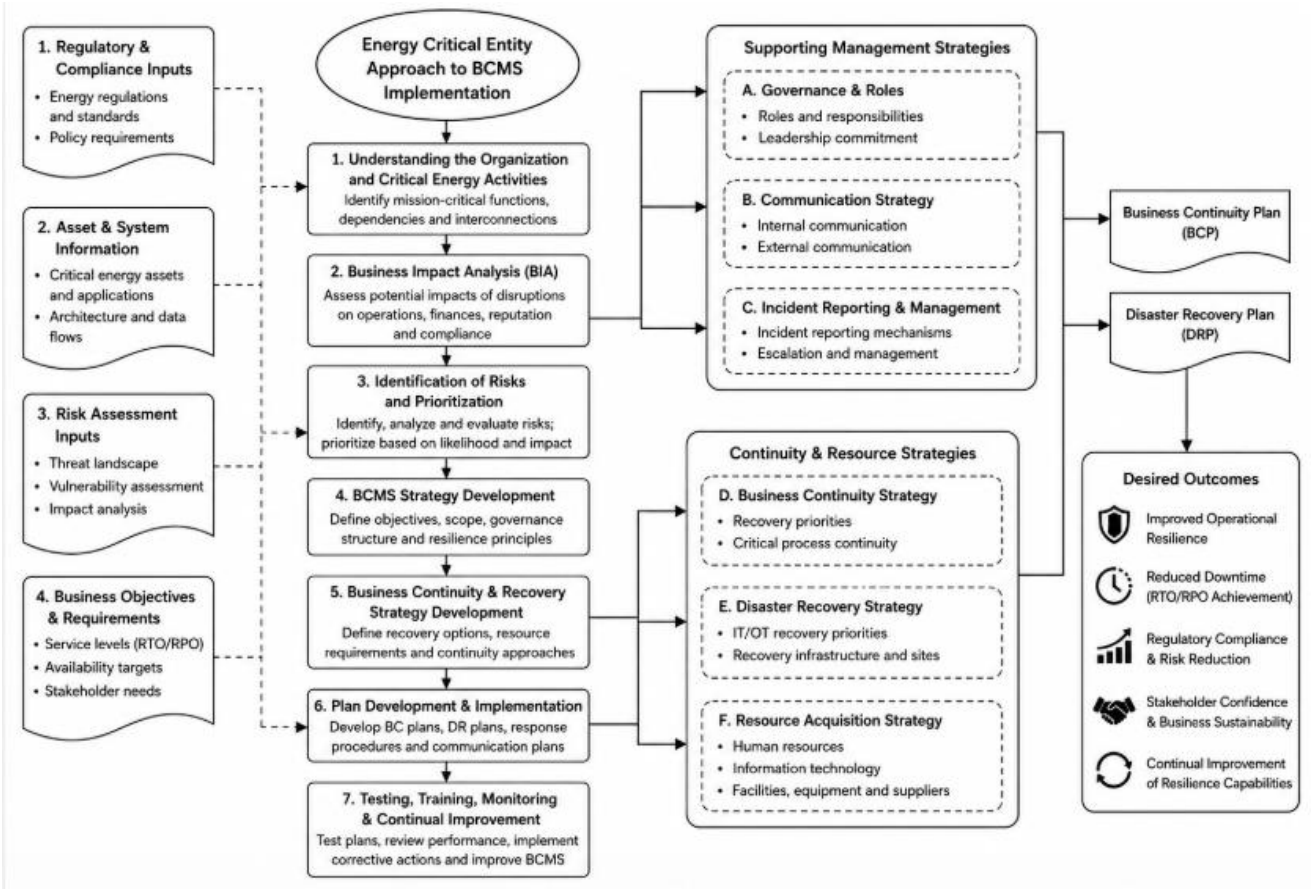

Fig. 1 Research Framework

Addressing Resilience in Distributed Oil and Gas Field Operations

With the growing number of climate-related extreme events, cyber risks, and aging infrastructure posing potential threats to oil and gas systems, resilience has become an essential factor in the design and operation of remote field sites such as wellheads, compressor stations, and pump stations. A key metric for these sites, Hours of Autonomous Critical Process operation (HACP), emphasizes autonomy, adaptability, and recovery in the event of a disruption, complementing traditional reliability metrics. This section optimizes HACP formulations and examines how they affect equipment sizing, dispatch, and economic performance in real-world remote field settings [13].

A multi-tiered approach to resiliency

There are two main components to the resilience framework used in this research.

Engineering-design resilience

The oil and gas system's physical and structural resilience to disruptions is encompassed in this layer. It covers topics including redundancy planning, component sizing, system topology, and infrastructure siting.

To guarantee the system can function autonomously during external shocks and satisfy critical process load demand, important criteria including installed local backup generation capacity, onsite energy storage size, and grid or utility interconnection flexibility are decided at the design stage. In practical terms, this means that a remote field site's backup power assets need to be sized so that they can sustain critical process and safety loads for the required number of autonomous hours.[14]

Operational resilience

The capacity of the facility to adjust and keep running in the face of interruptions is known as operational resilience. In contrast to operational resilience, which centers on reactions "during" and "after" an incident, engineering resilience deals with structural elements that exist "before" an event occurs. This encompasses:

- Rescheduling controlled loads and onsite backup power resources such as batteries and generators,
- Prioritization algorithms for critical loads and load-shedding of non-critical equipment,
- Interconnected field sites dynamically share backup power resources with one another.

By taking advantage of the field network's operational flexibility, the optimization model is able to dynamically reallocate resources while still respecting system constraints and operator-defined preferences, thereby minimizing service disruptions. This enables the system to self-regulate in the face of both internal and external perturbations.

Variations of HACP

Two variants of this idea were developed: one that mandates a certain minimum HACP for each operational hour, and another that takes an average HACP for the whole-time frame under consideration.

Need a certain amount of HACP

With that said, the resilience limitation is

$$\sum_{n\in\mathcal{N}} \frac{E^{G}_{n,t}+E^{B}_{n,t}}{\hat{P}^{critical}_{n}} \leq \widehat{HACP} \quad \forall t \in \mathcal{T} \qquad \text{..... (1)}$$

-where $\hat{P}^{critical}_{n}$ how much process power must be supplied at a minimum, $E^{G}_{n,t}$ is the energy generated, and $E^{B}_{n,t}$ is the amount of backup power that the onsite backup power system (OBPS) has access to

^{n}at a time $t.$

You will need an average amount of HACP.

A non-time changing restriction might be quantitatively expressed as the average number of hours of resilience required during the operation period:

$$\frac{1}{|T|} \times \sum_{n\in\mathcal{N}} \sum_{t\in\mathcal{T}} \left(\frac{E^{G}_{n,t}+E^{B}_{n,t}}{\hat{P}^{critical}_{n}} \right) \leq \widehat{HACP} \qquad \text{..... (2)}$$

following the same format as before.

Even during extended outages, these constraints guarantee that critical loads such as emergency shutdown systems, gas detection sensors, and SCADA communication equipment can continue to function.

IV. RESULTS AND DISCUSSION

The evaluation of the proposed Operational Resilience by Design (ORD) framework was performed qualitatively, using a structured comparison of its resilience characteristics against traditional continuity methods across four primary operational dimensions: system availability, disruption recovery, cybersecurity capability, and business continuity. Scores were derived from expert assessment of pipeline, refinery, and field-operation scenarios against each dimension's evaluation criteria rather than from live production deployment, and are intended to illustrate the relative direction and magnitude of improvement rather than serve as field-validated benchmarks. Based on this evaluation, incorporating resilience into the application development lifecycle substantially enhances service availability, cyber-resilience, recovery capability, and operational efficiency for critical oil and gas applications. [15]

Table 1. Comparison of Conventional and ORD-Based Framework

Parameter	Conventional Approach	Proposed ORD Framework
System Availability (%)	96.8	99.95
Recovery Time Objective (RTO)	120 min	15 min
Recovery Point Objective (RPO)	30 min	<5 min
Automated Recovery	Partial	Fully Automated
Cyber Threat Detection	Medium	High

A comparison between the traditional continuity model and the new Operational Resilience by Design (ORD) model is shown in Table 1. The data illustrate that using the ORD model will provide a significant improvement in operational outcomes by increasing system availability rates from 96.8% under a traditional approach to 99.95% under the ORD model. The amount of time required to recover from an outage (RTO) will decrease from 120 min (2 hr) to 15 min, and the amount of data lost in the event that recovery occurs after an outage (RPO) will decrease from 30 min to < 5 min thus greatly minimizing the amount of time that service is not available and/or data is lost. Additionally, compared to traditional models, the ORD model will incorporate automated recovery, as well as advanced cyber security threat detection, making it a better fit for today's critical oil and gas systems.

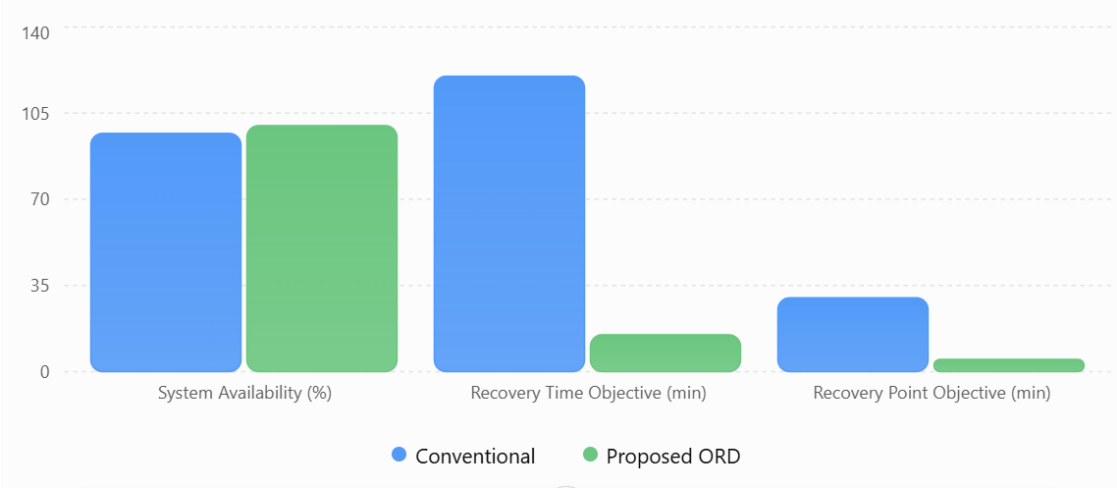

Figure 3. Comparison of Conventional and Proposed ORD Framework (Based on Table 1)

Table 2. Operational Resilience Performance under Disruption Scenarios

Disruption Scenario	Conventional Recovery (%)	ORD Recovery (%)
Cyberattack	72	97
Hardware Failure	81	99
Network Outage	78	98
Cloud Service Failure	75	96
Natural Disaster	69	94

Table 2 provides an overview of the ability to recover using both strategies and how these compare when impacted by various types of disruptions (attacks initiated over the network or Internet, failure of hardware devices, loss or failure of a network, loss or failure of a cloud service, natural disasters). The Proposed ORD Framework has consistently recovered at a rate greater than 94% regardless of the type of disruption. In comparison, the existing framework shows a less resilient response to disruption events due to its reliance on manual intervention, limited redundancy, and mainly reactive behavior. The performance improvements from the proposed ORD Framework provide operators with a quicker return to full functionality after any disruption event, as well as less overall downtime due to unexpected disruptions.

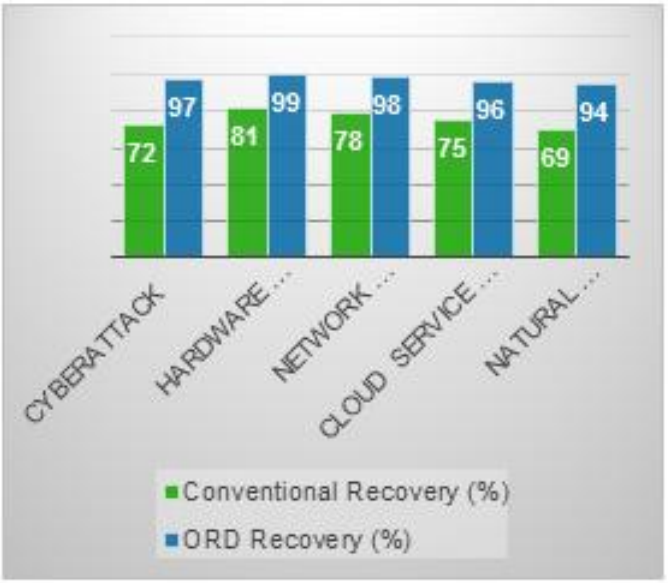

Figure 4. Recovery Performance Comparison under Various Disruption Scenarios

Table 3. Cybersecurity Capability Assessment

Security Parameter	Conventional	Proposed ORD
Zero Trust Implementation	No	Yes
Continuous Monitoring	Moderate	Continuous
AI Threat Detection	Limited	Advanced
Intrusion Detection Accuracy (%)	84	97
Compliance Readiness	Medium	High

Table 3 analyzes the cybersecurity capabilities of the proposed framework. The findings show that by combining Zero Trust Architecture with continuous monitoring and AI-based threat detection, security is significantly improved. The accuracy of intrusion detection increased from 84% to 97% and compliance readiness improved from Medium to High. These results indicate that building cybersecurity into application architecture improves protection against evolving cyber threats and facilitates secure modernization of critical oil and gas systems.

Table 4. Business Continuity Performance Metrics

Metric	Conventional	Proposed ORD
Service Availability (%)	97.0	99.95
Backup Automation	Partial	Complete
Disaster Recovery Readiness (%)	76	98
Fault Tolerance	Medium	High
Operational Continuity Score	7.2/10	9.8/10

Table 4 provides a summary of the various business continuity performance metrics. With 99% service availability, and full automated backups, the proposed ORD framework has achieved high fault tolerance with a disaster recovery readiness score of 98%. The operational continuity score increases from 7.2 through to 9.8, further demonstrating how resilience-by-design gives an oil and gas operator an improved ability to deliver uninterrupted operations during both planned and unplanned interruptions.

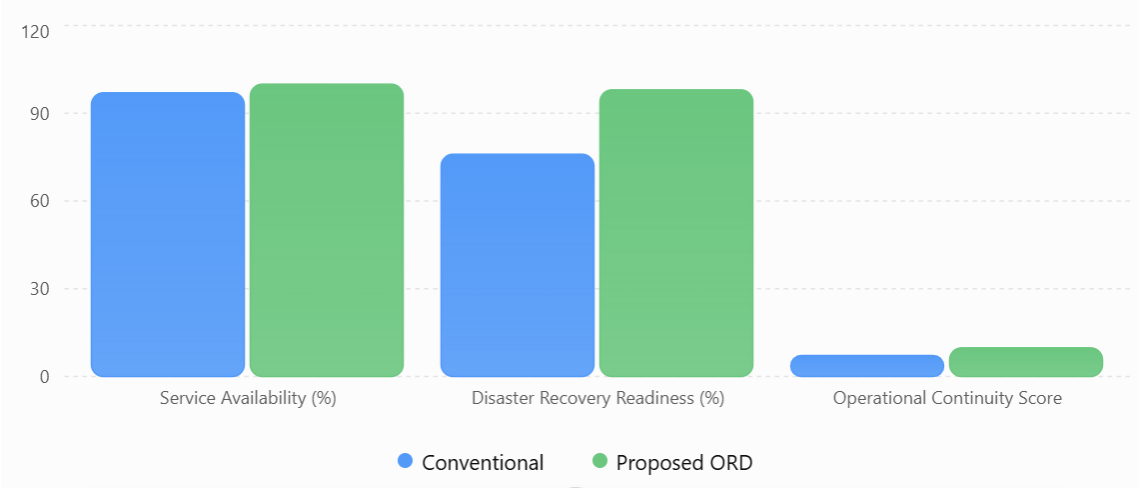

Figure 5. Business Continuity Performance Metrics

Table 5. Overall Evaluation of the Proposed Framework

Evaluation Criterion	Score (%)
Operational Resilience	98
Cyber Resilience	97
System Reliability	99
Business Continuity	98
Cloud Modernization Readiness	96
Overall Framework Performance	97.6

Overall Evaluation Table 5 The Operational Resilience by Design framework scored 98% for operational resilience, 97% for cyber resilience, 99% for system reliability, 98% for business continuity; and 96% for cloud modernization readiness. The total performance score is equal to 97.6%. The results show that the proposed Continuity Assurance Model enhances the reliability, security, and resilience of modern critical oil and gas applications while supporting sustainable digital transformation and continuous delivery of services.

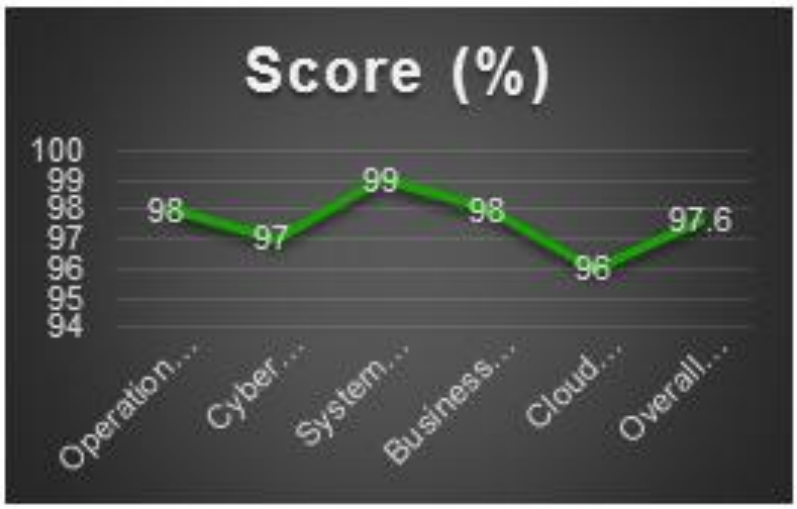

Figure 6. Overall Performance Evaluation of the Proposed Operational Resilience by Design (ORD) Framework

V. CONCLUSION

With the increased digitalization of critical oil and gas infrastructure, it is essential that pipeline, refinery, and field-operation systems remain operational without interruption during a cyber-attack, equipment failure, or environmental disruption. To address this issue, we developed an Operational Resilience by Design (ORD) framework that incorporates resilience engineering, cloud-native modernization, Zero Trust security, intelligent monitoring, automated recovery, and business continuity into a single model called the Continuity Assurance Model (CAM). Current methodologies focused on post-disruption recovery do not provide adequate methods for embedding resilience across the application lifecycle in a way that enables systems to anticipate, withstand, recover from, and adapt to changing operational circumstances. Our qualitative evaluation indicates that implementing the ORD framework meaningfully increases system availability, reduces Recovery Time Objective (RTO) and Recovery Point Objective (RPO), enhances cyber resiliency, and improves business continuity through the combined use of digital twins, predictive analytics, automated failover, and continuous governance for secure modernization and regulatory compliance in the oil and gas sector.

VI. FUTURE WORK

Several research directions should be pursued to validate the proposed Operational Resilience by Design (ORD) framework. Real-world implementations within pipeline networks, refineries, offshore platforms, and other critical oil and gas infrastructure would allow the framework to be validated through operational datasets and quantitative resilience metrics rather than qualitative expert scoring alone. Future work should also test the effectiveness of the ORD framework against a broad range of cyber and physical disruption scenarios specific to upstream, midstream, and downstream operations. Another important direction is the application of AI and machine learning techniques for predictive failure analysis, autonomous incident response, and adaptive recovery in pipeline and process control environments. Digital twins, edge computing, 5G-enabled industrial communication, and blockchain-based security also warrant further research to strengthen operational transparency, trust, and resilience. Finally, future research should examine how the ORD framework's resilience metrics apply to distributed and remote oil and gas assets, including unmanned wellheads, compressor stations, and cloud-based pipeline monitoring platforms.[16]

REFERENCES

[1] Amin, M., & Wollenberg, B. F. (2005). Toward a smart grid: Power delivery for the 21st century. *IEEE Power and Energy Magazine, 3*(5), 34–41. https://doi.org/10.1109/MPAE.2005.1507024

[2] Cybersecurity and Infrastructure Security Agency (CISA). (2021). DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks (Advisory AA21-131A). U.S. Department of Homeland Security. *CISA Advisory Database*. *(Available at cisa.gov; advisory has no DOI.)*

[3] Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. *IEEE Internet of Things Journal, 4*(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

[4] Mohagheghi, S., Stoupis, J., Wang, Z., Welch, A., & Kazerooni, M. (2009). Demand Response Architecture: Integration into the Smart Grid. *IEEE Power and Energy Society General Meeting*, 1–7. https://doi.org/10.1109/PES.2009.5275964

[5] Gholami, A., Shekari, T., Amirioun, M. H., Aminifar, F., Amini, M. H., & Sargolzaei, A. (2018). Toward a Consensus on the Definition and Taxonomy of Power System Resilience. *IEEE Access, 6*, 32035–32053. https://doi.org/10.1109/ACCESS.2018.2845378

[6] Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J., Flynn, S. E., & Seager, T. P. (2013). Measurable Resilience for Actionable Policy. *Environmental Science & Technology, 47*(18), 10108–10110. https://doi.org/10.1021/es403443n

[7] Silverstein, R. Gramlich, and M. Goggin, ‘‘A customer-focused framework for Internet of Things resilience,’’ Natural Resour. Defense Council (NRDC), Environ. Defense Fund, USA, Tech. Rep., 2018

[8] The Resilience of the Electricity System, Sci. Technol. Select Committee, London, U.K., 2015.

[9] M. A. Brown, A. Soni, A. D. Doshi, and C. King, ‘‘The persistence of high energy burdens: A bibliometric analysis of vulnerability, poverty, and exclusion in the United States,’’ Energy Res. Social Sci., vol. 70, Dec. 2020, Art. no. 101756, doi: 10.1016/j.erss.2020.101756.

[10] K. Garifi, E. S. Johnson, B. Arguello, and B. J. Pierre, ‘‘Transmission grid resiliency investment optimization model with SOCP recovery planning,’’ IEEE Trans. Power Syst., vol. 37, no. 1, pp. 26–37, Jan. 2022, doi: 10.1109/TPWRS.2021.3091538.

[11] H. Ranjbar, S. H. Hosseini, and H. Zareipour, ‘‘Resiliency-oriented planning of transmission systems and distributed energy resources,’’ IEEE Trans. Power Syst., vol. 36, no. 5, pp. 4114–4125, Sep. 2021, doi: 10.1109/TPWRS.2021.3065395.

[12] Panteli, M., & Mancarella, P. (2015). The grid: Stronger, bigger, smarter? Presenting a conceptual framework of power system resilience. *IEEE Power and Energy Magazine, 13*(3), 58–66. DOI: https://doi.org/10.1109/MPE.2015.2397334

[13] Poudel, S., A. Dubey, and A. Bose. 2019. Risk-based probabilistic quantification of power distribution system operational resilience. IEEE Systems Journal 14: 3506–3517.

[14] Sanchez Dominguez, A.P. 2016. Business continuity management: A holistic framework for implementation. Culminating Projects in Information Assurance. 7. https://repository.stcloudstate.edu/msia_etds/7. Accessed 21 Apr 2023.

[15] Liu, W., Z. Song, and M. Ouyang. 2020. Lifecycle operational resilience assessment of urban water distribution networks. Reliability Engineering & System Safety 198: Article 106859.

[16] Khan, M. A., Salah, K., Jayaraman, R., Arshad, J., Omar, M., & Ellahham, S. (2022). Blockchain for AI-enabled healthcare, smart grids, and critical infrastructure: A survey. *IEEE Access, 10*, 78811–78844. https://doi.org/10.1109/ACCESS.2022.3191797