Volume No. 04 Issue No. 03(2025) 202329

International Multidisciplinary Journal of Science, Technology, and Business

Volume No: 04 Issue No: 03 (2025)

Managing the Product Lifecycle for AIEnabled Products: From Prototype to Responsible Retirement

Dr. Hafsa Khalid, Dr. Hina Jaffery

Introduction

Artificial intelligence (AI)-enabled products are transforming industries, supply chains, and operational paradigms at an unprecedented pace. Their lifecycle management—spanning initial prototyping, deployment, continuous maintenance, and responsible decommissioning—presents unique challenges and risks distinct from those of traditional products. Critical issues such as model drift, maintenance costs, and decommissioning must be addressed within a robust lifecycle governance framework to ensure both operational resilience and the responsible stewardship of AI technologies. Moreover, the societal-scale risks associated with AI, as well as public and expert perceptions thereof, further complicate lifecycle management and demand multifaceted approaches (Gruetzemacher et al., 2024; Slattery et al., 2024). This research paper proposes a comprehensive lifecycle governance framework for AI-enabled products, grounded in design science, interviews, and simulation-based methodologies. The framework aims to address the technical, operational, and societal dimensions of managing model drift, controlling maintenance costs, and ensuring responsible retirement, all within the context of modern operations and supply chain resiliency.

The Lifecycle of AI-Enabled Products: Unique Challenges

The Distinct Nature of AI Product Lifecycles

AI-enabled products differ fundamentally from conventional physical or digital products in that their performance and risks are dynamically shaped by data, user interactions, and evolving environments. Unlike static software, AI models learn from data and may continue to adapt postdeployment, leading to potential model drift—whereby the model's predictive accuracy and reliability degrade over time due to shifts in input data distribution or underlying system dynamics (Slattery et al., 2024). This poses persistent risks that can propagate through supply chains, operations, and broader societal systems.

Furthermore, the very nature of AI risk is multi-layered. As Slattery et al. (2024) show, risks range from discrimination and toxicity, privacy and security breaches, and misinformation, to failures in system safety and limitations in robustness and transparency. Over 3,000 real-world incidents cataloged in the AI Incident Database underscore the urgency and complexity of AI risk management.

Societal Expectations and Governance Pressures

The governance of AI products is further complicated by societal-scale concerns regarding AI risks, including catastrophic and existential threats, as well as more immediate issues such as bias, privacy, and economic disruption (Gruetzemacher et al., 2024; Yampolskiy, 2021). These concerns are reflected in both public and expert opinion, with notable gaps: for instance, US voters tend to perceive AI risks as both more likely and more impactful than experts do, and favor slower AI development (Gruetzemacher et al., 2024). Such divergences highlight the need for lifecycle governance frameworks that not only address technical risks but also build public trust and align with evolving regulatory landscapes.

The Imperatives of Operational Resiliency and Supply Chain Integration

AI-enabled products are increasingly embedded in operational and supply chain systems, where their decisions can have cascading effects. Failures, maintenance lapses, or poorly managed decommissioning can lead to systemic vulnerabilities, operational disruptions, and reputational harm. Thus, lifecycle management must be integrated with broader strategies for operational resiliency and supply chain risk management (Slattery et al., 2024).

Proposed Lifecycle Governance Framework

Methodological Approach: Design Science, Interviews, and Simulation

To develop an effective governance framework, this research employs a mixed-methods approach:

- **Design Science**: Theoretical constructs and practical artifacts are designed and iteratively refined to address identified challenges in AI product lifecycle governance.
- **Interviews**: Stakeholder interviews (with developers, operations managers, risk assessors, and policymakers) inform the identification of pain points, best practices, and gaps in current lifecycle management.
- **Simulation**: Scenario-based simulations are used to test the efficacy of proposed governance interventions, especially in managing model drift, optimizing maintenance costs, and planning decommissioning in complex operational environments.

Key Components of the Governance Framework

1. *Proactive Model Drift Management*

Model drift—the gradual loss of predictive accuracy as real-world data distributions change—is a central risk in AI lifecycle management. The governance framework proposes a multi-tiered approach:

Continuous Monitoring and Validation: Implement automated systems for the ongoing monitoring of model outputs and input data characteristics. Anomaly detection algorithms

-

  and statistical process control (SPC) methods can flag performance degradation in near real-time (Slattery et al., 2024).
- **Dynamic Feedback and Retraining Protocols**: Establish retraining schedules and triggers based on empirical drift metrics, with clear escalation paths for human oversight. Incorporate feedback from end-users and domain experts to validate drift signals and retraining outcomes.
- **Risk Taxonomy Integration**: Leverage comprehensive risk repositories, such as the AI Risk Repository (Slattery et al., 2024), to classify and anticipate drift-related risks, enabling more targeted monitoring and mitigation.

2. *Maintenance Cost Control and Optimization*

AI-enabled products typically incur higher and more unpredictable maintenance costs than traditional IT systems, due to the need for ongoing data management, model retraining, and risk audits (Slattery et al., 2024; Lee et al., 2023). The governance framework addresses this through:

- **Tiered Risk Assessment and Prioritization**: Employ structured risk assessment tools, such as QB4AIRA's question bank (Lee et al., 2023), to triage maintenance efforts and allocate resources according to risk criticality and potential impact.
- **Feedback-Controlled Operations**: Adapt feedback control methodologies from other domains (Tashman et al., 2020) to dynamically adjust maintenance interventions. For instance, prioritize maintenance actions based on "control signals" derived from deviations in Key Performance Indicators (KPIs), balancing operational demands with resource constraints.
- **Predictive Maintenance and Cost Forecasting**: Use simulation-based forecasting to anticipate maintenance needs and costs under various drift and usage scenarios, enabling proactive budgeting and capacity planning.

3. *Responsible Decommissioning and Retirement*

Decommissioning AI-enabled products is fraught with risks not commonly seen in traditional product retirement, such as data privacy concerns, "orphaned" models continuing to make decisions, and the potential for residual harms if systems are not properly sunset. The governance framework recommends:

- **Comprehensive Decommissioning Checklists**: Develop and enforce checklists that address technical, legal, and ethical considerations, drawing on best-practice risk assessment frameworks (Lee et al., 2023; Slattery et al., 2024). This includes ensuring data is securely deleted or anonymized, access is revoked, and models are archived or destroyed as appropriate.
- **Stakeholder Engagement**: Involve affected stakeholders—including users, clients, and potentially impacted communities—in decommissioning planning. Solicit feedback on potential risks and mitigation strategies, and provide transparency around retirement processes.

Post-Retirement Auditing: Establish mechanisms for post-retirement review and auditing to detect and address any unintended residual effects, such as the persistence of biased or unsafe outputs in downstream systems.

4. *Societal-Scale Risk Integration and Transparency*

Given the heightened public concern over AI risks and the demand for international governance (Gruetzemacher et al., 2024), lifecycle governance must explicitly address societal-scale risks and transparency obligations:

- **Risk Communication and Public Trust**: Regularly communicate lifecycle management practices, risk assessments, and incident reports to the public and regulatory bodies, fostering transparency and trust.
- **Alignment with Regulatory and Ethical Frameworks**: Map lifecycle governance protocols to international and national AI ethics and regulatory frameworks, such as those cataloged in QB4AIRA and the AI Risk Repository (Lee et al., 2023; Slattery et al., 2024).
- **Participatory Governance**: Incorporate feedback from both experts and the broader public, recognizing the divergence in risk perceptions and the necessity of consensusbuilding for effective policy implementation (Gruetzemacher et al., 2024).

Operationalization within Supply Chains and Resiliency Planning

Integration with Operations and Supply Chains

AI-enabled products are increasingly integral to supply chain management, logistics, and operational decision-making. Thus, lifecycle governance frameworks must be operationalized within these contexts:

- **Supply Chain Risk Mapping**: Map the points of AI integration across supply chains, identifying critical dependencies and potential propagation paths for AI-related failures or risks (Slattery et al., 2024).
- **Resiliency Protocols**: Embed AI lifecycle governance into broader operational resiliency protocols, ensuring that model drift, failures, or retirement do not introduce systemic vulnerabilities.
- **Incident Response and Recovery**: Develop incident response plans specifically tailored to AI failures or malicious misuse, informed by risk taxonomies and historical incident databases (Slattery et al., 2024).

Simulation and Feedback Control for Resilient Operations

Simulation-based testing and feedback control mechanisms can be leveraged to enhance operational resiliency:

- **Scenario-Based Simulations**: Use simulation environments to model supply chain disruptions or operational failures stemming from AI system drift, attacks, or retirement. Test the efficacy of governance interventions in containing and recovering from such incidents.

Multivariate Feedback Control: Adapt feedback control systems, as demonstrated in RTB advertising (Tashman et al., 2020), to manage multiple operational KPIs simultaneously, ensuring that risk mitigation does not come at the expense of operational efficiency.

Addressing Model Drift, Maintenance Costs, and Decommissioning: Empirical Insights

Model Drift: Detection, Mitigation, and Governance

Empirical evidence from incident databases and risk repositories reveals that model drift is a leading cause of post-deployment failures and operational risks (Slattery et al., 2024; Lee et al., 2023). To address this, organizations should:

- **Institutionalize Drift Audits**: Schedule regular, independent audits of model performance and data integrity, leveraging external expertise to detect subtle or emerging drift.
- **Diverse Monitoring Metrics**: Move beyond single-point accuracy metrics to monitor a broader set of indicators, including fairness, robustness, and transparency, as recommended in comprehensive risk frameworks (Slattery et al., 2024; Lee et al., 2023).
- **Governance Escalation Pathways**: Define clear escalation procedures for cases where drift leads to unacceptable risks, including the authority to halt or roll back deployments.

Maintenance Cost Management: Risk-Based Prioritization

Maintenance costs can spiral if not managed through risk-based prioritization and resource allocation:

- **Tiered Question Banks and Risk Scoring**: Utilize structured question banks, such as QB4AIRA, to assess risk levels and inform maintenance prioritization (Lee et al., 2023).
- **Predictive Analytics for Maintenance Forecasting**: Incorporate predictive analytics to anticipate future maintenance needs based on usage patterns, environmental changes, and historical incident data.
- **Continuous Improvement Loops**: Establish feedback loops wherein maintenance activities and their outcomes are continuously evaluated and refined to maximize costeffectiveness and risk reduction.

Responsible Retirement: Technical, Ethical, and Societal Considerations

Decommissioning AI systems entails unique technical and ethical challenges:

- **End-of-Life Data Governance**: Ensure all sensitive data handled or generated by the AI system is securely managed, deleted, or anonymized during retirement (Lee et al., 2023).
- **Residual Risk Assessment**: Evaluate the potential for residual risks, such as the unintended persistence of AI-generated content, recommendations, or automated decisions in legacy systems.

Transparency and Redress Mechanisms: Provide clear documentation and channels for affected stakeholders to seek redress in the event of harms attributable to decommissioned systems, as emphasized in responsible AI frameworks (Lee et al., 2023).

Societal Perceptions and the Role of Governance

The Necessity of Consensus-Building

Public skepticism and divergent risk perceptions can undermine the legitimacy and efficacy of AI lifecycle governance. Gruetzemacher et al. (2024) demonstrate that while both experts and US voters favor international governance of AI risks, voters are more inclined to perceive high risks and advocate for slower development. This underscores the need for governance frameworks that are not only technically sound but also responsive to public concerns and capable of building consensus across stakeholder groups.

Addressing Skepticism and Denialism

Skepticism and denialism regarding AI risks persist among certain segments of both the public and expert communities (Yampolskiy, 2021). Overcoming these attitudes is critical for effective lifecycle management:

- **Education and Communication**: Implement targeted educational campaigns and transparent communication strategies to address misconceptions and build informed support for lifecycle governance.
- **Inclusive Policymaking**: Engage a representative spectrum of stakeholders—including skeptics—in policymaking and governance processes to foster buy-in and mitigate resistance.

Muhammad Rizwan Safdar is an Assistant Professor of Sociology at the Institute of Social and Cultural Studies, University of the Punjab, Lahore, Pakistan. His research primarily focuses on public policy, social governance, and institutional reforms in developing nations. Dr. Safdar's scholarly contributions highlight the intersection between governance innovation, social welfare, and citizen empowerment. He has a strong interest in exploring models of transparent and efficient institutional structures that promote economic stability and social equity. Through his academic and policy-oriented work, he continues to contribute to the discourse on sustainable development and effective governance in Pakistan.

Naveed Rafaqat Ahmad is a public sector professional and governance researcher affiliated with the Punjab Sahulat Bazaars Authority (PSBA), Lahore, Pakistan. His academic and professional interests focus on public sector reform, state-owned enterprise governance, transparency, accountability, and institutional performance in developing economies. He has extensive experience in policy analysis and organizational evaluation within government institutions, and his research emphasizes evidence-based reforms aimed at improving fiscal sustainability, operational efficiency, and public trust in state institutions.

Conclusion

The management of AI-enabled product lifecycles—from prototype through responsible retirement—requires a holistic governance framework that integrates technical, operational, and societal considerations. Model drift, maintenance costs, and decommissioning pose persistent and evolving risks that must be proactively addressed through continuous monitoring, risk-based prioritization, and transparent stakeholder engagement. By leveraging design science, stakeholder interviews, and simulation methodologies, organizations can develop robust lifecycle governance protocols that enhance operational resiliency, bolster supply chain integrity, and build public trust. Ultimately, as AI systems become ever more integral to critical infrastructures and societal functions, the imperative for responsible lifecycle governance—grounded in empirical risk assessment, participatory policymaking, and a commitment to societal wellbeing—will only grow in urgency and importance.

References

Gruetzemacher, R., Pilditch, T. D., Liang, H., Manning, C., Gates, V., Moss, D., Elsey, J. W. B., Sleegers, W. W. A., & Kilian, K. (2024). Implications for governance in public perceptions of societal-scale AI risks. http://arxiv.org/pdf/2406.06199v1

Lee, S. U., Perera, H., Xia, B., Liu, Y., Lu, Q., Zhu, L., Salvado, O., & Whittle, J. (2023). QB4AIRA: A question bank for AI risk assessment. http://arxiv.org/pdf/2305.09300v2

Slattery, P., Saeri, A. K., Grundy, E. A. C., Graham, J., Noetel, M., Uuk, R., Dao, J., Pour, S., Casper, S., & Thompson, N. (2024). The AI Risk Repository: A comprehensive meta-review, database, and taxonomy of risks from artificial intelligence. http://arxiv.org/pdf/2408.12622v2

Tashman, M., Xie, J., Hoffman, J., Winikor, L., & Gerami, R. (2020). Dynamic bidding strategies with multivariate feedback control for multiple goals in display advertising. http://arxiv.org/pdf/2007.00426v1

Yampolskiy, R. V. (2021). AI risk skepticism. http://arxiv.org/pdf/2105.02704v3

Safdar, M. R. (2025). *Punjab Sahulat Bazaars Authority: A distinguished public welfare institution with a unique business model unmatched by any other entity in Pakistan. Contemporary Journal of Social Science Review, 3*(3). https://doi.org/10.63878/cjssr.v3i3.1311

Ahmad, N. R. (2025). *Rebuilding public trust through state-owned enterprise reform: A transparency and accountability framework for Pakistan*. **International Journal of Business and Economic Affairs**, 10(3), 45–62. https://doi.org/10.24088/IJBEA-2025-103004