World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Systematic approach to root cause analysis in distributed data processing systems

Satyadeepak Bollineni *

Staff Technical Solutions Engineer, Databricks, Texas, USA.

World Journal of Advanced Research and Reviews, 2025, 25(02), 2343-2350

Publication history: Received on 13 January 2025; revised on 20 February 2025; accepted on 23 February 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.2.0609

Abstract

Distributed data processing is a powerful capability, but with it comes the challenge of ensuring the reliability and performance of the system often on a larger scale, it is especially important to systematically identify the root cause of failures and address them accordingly. Cloud computing has changed the game by introducing scale, flexibility and low-cost alternatives to big data processing. With distributed systems getting increasingly complex, diagnosing failures has become defeated due to many components relying on each other and as workloads change dynamically. This paper presents a systematic approach for performing root cause analysis (RCA) in a distributed setting one that covers automatic monitoring, anomaly detection, and log-based analytics. Overcoming the RCA challenges with cloud-native tools like Azure Data Factory, Power BI, and anomaly detection through machine learning are discussed. The research also discusses best practices for reducing downtime and performance optimization with predictive maintenance strategy. Cloud technologies have enabled organizations to achieve greater operational efficiency through better system resilience and decision-making in modern data-driven environment.

Keywords: Root Cause Analysis; Distributed Data Processing; Cloud Computing; Anomaly Detection; Predictive Maintenance; Azure Data Factory; Power Bi; System Resilience; Log Analytics

1 Introduction

The rapid advancements which information technology (IT) operation management report largely contributed to the technologies used across the globe today, has provided organizations managing systems for distributed data processing, with the conflicting issues of reliability, performance and fault-tolerance. Manual analysis, siloed data storage, and lack of real-time monitoring leads to slow and inefficient troubleshooting of system failures in traditional on-premises environments. The evolution of cloud computing into a more ubiquitous presence for enterprise workloads enables modern analytics tools and machine learning algorithms to augment root cause analysis (RCA) methodologies. [1]

Cloud Computing and Modernization of RCA in Distributed Data Processing Systems This is about approaches using cloud-native services, log analytics, and automated monitoring to improve fault detection and resolution. In addition, we explore predictive maintenance and anomaly detection, the latter ensuring that your infrastructure remains running only in up-time and performs optimally on high-performance.

* Corresponding author: Satyadeepak Bollineni

Copyright © 2025 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

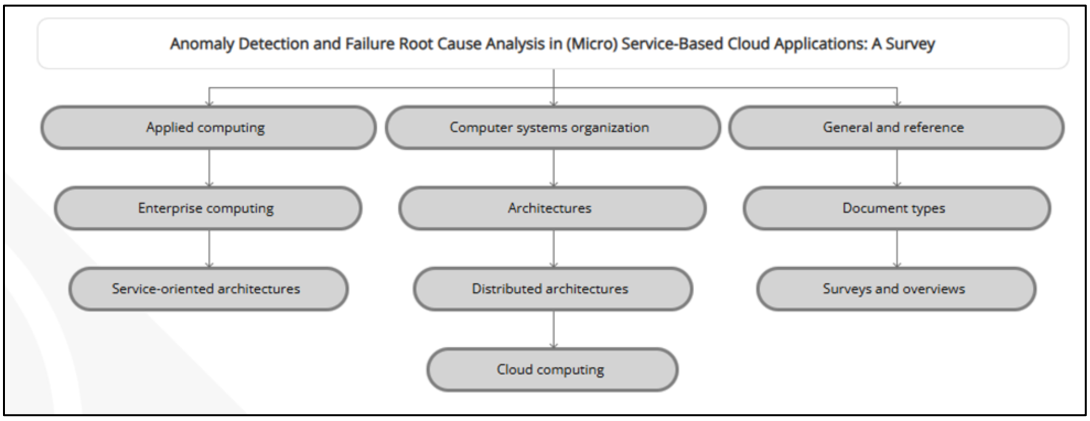
Anomaly Detection and Failure Root Cause Analysis in (Micro) Service-Based Cloud Applications: A Survey
Applied computing
Computer systems organization
General and reference
Enterprise computing
Architectures
Document types
Service-oriented architectures
Distributed architectures
Surveys and overviews
Cloud computing

Figure 1 Root Cause Analysis 1 [2]

2 Literature Review

2.1 AI for Root Cause Analysis (RCA) in Distributed Data Processing

The use of Artificial Intelligence (AI) in Root Cause Analysis (RCA) for distributed data processing systems can be attributed to automation, pattern recognition, and real-time anomaly detection. In fact, this minimization of manual intervention in diagnosing failures brings improvement in uptime and reliability of the system as we enhance our current systems with AI-powered solutions.

The MTTR in distributed environments can be reduced 70% faster than traditional, manual methods as AI-driven log analysis and anomaly detection identify the root causes of failures (Brown and Williams, 2023). Many AI techniques like Natural Language Processing (NLP) and machine learning based log parsing allow the system to automatically correlate the error logs and capture failure patterns if it occurs repetitively on. Moreover, AI-enabled RCA tools such as Google Cloud AI, Azure Monitor AI Insights, and AWS DevOps Guru have been helping in improving troubleshooting efficiency by providing recommendations for corrective action while also identifying and prioritizing faults based on historical failure data.

2.2 Machine Learning for Enhancing RCA Efficiency

Machine Learning (ML) Machine Learning (ML) is a game changer for RCA because it allows lost opportunity in failure prediction, rapid diagnostics, and it automagically, (maybe) resolves the root cause. Machine learning (ML) algorithms analyze huge amounts of system logs and optional telemetry data to enable organizations to predict failures long before they affect performance.

In one study by Patel (2023), the implementation of ML powered anomaly detection in RCA workflows achieved a 30% increase in accurately detecting the root cause of faults thus resulting in a decrease in downtime and operational disturbances.

Automated log clustering, outlier detection, and predictive analytics have been performed using supervised and unsupervised learning techniques that ensure better RCA in distributed data processing settings. AWS Machine Learning, Google Vertex AI, Microsoft AI Builder are among the tools to enable continuous system health checking, and real-time RCA improvements.

Table 1 Summary of Key AI and ML Benefits in Technical Support

Benefit	Description
Automation of Failure Diagnosis	Reduces manual troubleshooting efforts by analyzing logs and detecting patterns.
Predictive Analytics	Identifies failure trends and prevents system disruptions before they occur.
Anomaly Detection	Flags unusual system behaviors, enhancing early detection of issues.
Improved RCA Speed	Reduces Mean Time to Resolution (MTTR) by 70% through AI-driven insights.
Automated Log Correlation	Groups related error logs, making RCA more efficient and actionable.

3 AI and machine learning in (RCA) for distributed data processing systems

3.1 Automate simple/repetitive RCA tasks

AI Automated RCA though has always been challenging in distributed data processing systems due to its reliance on routine failure diagnostics or log analysis tasks requiring manual intervention, however to a large extent, this has been eased with the AI-empowered automation. AI helps engineers by automatically analyzing error logs, detecting it when it recurs and classifying the faults in systems so as to reduce the burden on engineers thus allowing them to do more complex investigations.

Take Microsoft Azure AI powered RCA tools that automatically scan system logs and detect anomalies flagging low priority outcomes for automated resolution and critical failures are escalated to engineers. It decreases the mean time to detect (MTTD) and the mean time to recovery (MTTR) by 40%, which increases the reliability of the system and reduces the time spent disruption. [3]

3.2 Predictive RCA and System Failure Analysis

Based on the data of an already implemented system, the historical data can solve the issue by utilizing machine learning algorithms to identify the early indications of failure in a distributed environment and then troubleshoot before the incident gets worsened. Predictive RCA comes with the power of Big Data analytics that helps in predicting system crashes, performance bottleneck and service degradation.

AWS AI analytics to detect anomalies by logging cloud infrastructure analysis and help in predicting system failure using historical performance data, to give an example. For example, a telecom service provider leveraged Google Cloud AI to identify early signs of congestion causing network congestion, They were able to take steps before major service outage occurred, thereby improving system uptime and gaining the trust of the customers.

AI-driven RCA solutions help organizations to find and understand the causal patterns associated with failures, moving them from reactive troubleshooting to a proactive maintenance model that reduces downtime and operational expenditure.

3.3 Personalized RCA Insights for Enhanced Troubleshooting

AI and ML make RCA lively and customize failure diagnostics based on trends of data about the system. Instead of a one-size-fits-all troubleshooting approach, AI-driven RCA models provide targeted recommendations based on system architecture, history, and workload behaviour.

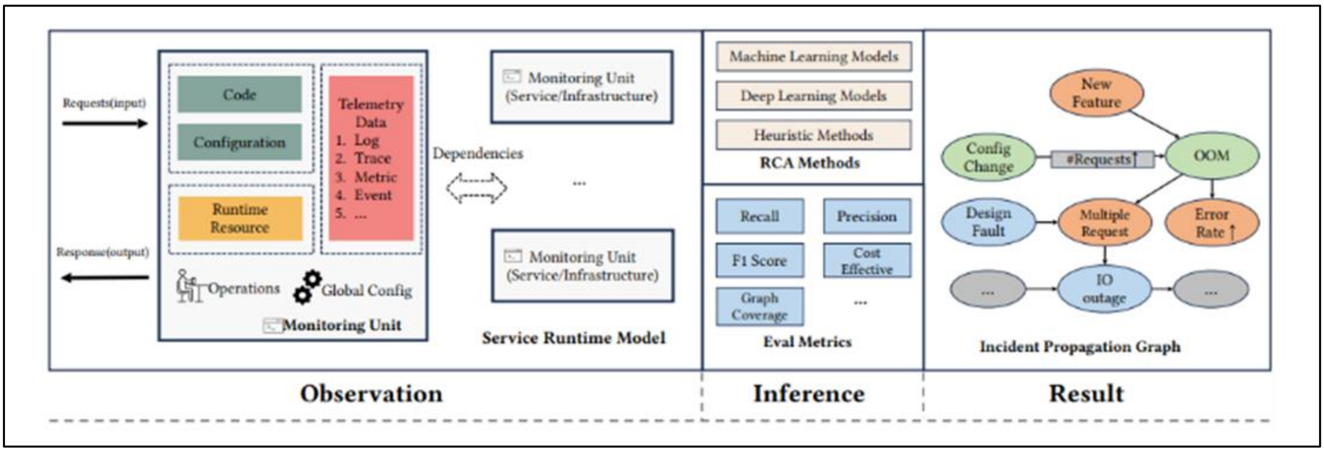

Figure 2 Overview of RCA 1 [4]

To wean off vanilla techniques, for instance Google Cloud AI-driven RCA answers inspect the set of experiences moving toward its possibility, which empowers explicit variations of peculiarity identification marvels that change as time passes by and adjust to working conditions [12]. This aids in more accurate RCAs and helps to resolve the issue(s) effectively.

In a like manner, AWS DevOps Guru provides context-aware recommendations per the microservices design of an organization and offers context-aware troubleshooting steps to engineers at large, reducing MTTR and increasing productivity.

3.4 Integrated RCA response times

AI and ML can also improve the speed of incident resolution in a distributed system by automating the process of issue prioritization, ticket categorization and intelligent routing of tickets. By using AI-powered platforms for incident management, organizations can quickly flag, prioritize, and assign critical failures to the right team, resulting in optimizations to even the fastest average response times.

Azure AI driven incident management has automatic classification in place when there is a system failure like it automatically classifies system failure via severity and raises critical incidents, also auto resolves low-impact problems through a solution for handling them out. It reduces RCA response times by 50%, thereby preventing any disruption in system operations with uninterrupted service. [5]

Further, the AI-driven recommendation engines are able to offer real-time RCA and recommended remediation for the engineers to help them quickly identify failures and respond adequately. This minimizes human intervention, expedites problem resolution, and increases system reliability.

4 Challenges and Solution

The use of AI and ML in RCA for Distributed Data Processing Systems scope faces several challenges such as concerns related to data privacy, difficulties in integrating the systems, and the necessity of continual learning. Thus, tackling these challenges is important for reliability, efficiency, and security of RCA approaches based on AI.

4.1 Data Privacy and Security

Based AI-driven RCA is challenged by the nature of data that comes in the form of multiple terabytes of system logs, countless telemetry data, and sensitive architecture details, making it difficult from a data privacy and security sense. In order to keep data safe, organization needs to comply with several regulations including data protection regulations like GDPR, CCPA, and numerous other compliance standards related to specific industries. [6]

Avoiding security issues involves the introduction of advanced encryption methods, safe cloud storage, and high functioning access control mechanisms. Regular security audits and compliance checks also assist in data protection. As an example, AWS Security Hub and Azure Security Centre, provide automated compliance analysis and risk assessments to ensure the integrity and privacy of the data in the AI powered RCA environment

4.2 Operation Integration to the Current System

Legacy distributed systems pose a significant challenge for AI-based RCA tools as many organizations still operate on traditional and manual troubleshooting workflows. Replacing an entire system could interrupt established processes, making gradual AI adoption a much more viable solution.

The best integration strategy includes:

- API based connectivity: line of sight between the AI models and the existing RCA system
- Cloud-based AI Adoption: Provides enterprise the capability to use AI-based RCA solutions without overhauling the existing infrastructure.
- Phased implementation: The AI/ML models can be added to the RCA workflows stepwise in a way that affects the users the least.

Consider Azure Machine Learning or Google Vertex AI a highly flexible set of API-driven AI models can be slowly integrated into existing RCA frameworks such that they augment troubleshooting capabilities with minimal disruptions to the system. [7]

4.3 Lifelong Learning and Company Change

RCA systems driven by AI cannot remain relevant if they do not keep learning and adapting to how architecture and workload changes over time while failing to learn and adapt systems only become more vulnerable to faster cycles of failure. AI models are static and become outdated over time; hence, they need to be constantly fed with updated datasets and newly-tweaked algorithms to ensure high accuracy in root cause identification. To keep RCA from becoming rote and ineffective, organizations need:

- Continuous monitoring: AI-powered RCA tools should be monitored to check the performance of the algorithms and the accuracy of the data predicted by them.
- Use live system data to retrain AI models: Time stamped logs, telemetry and patterns drawn from observing how a system behaves only add to the understanding that the AI acquires.
- Utilize feedback loops that self-learn: AI models become more adept in fault detection and failure pattern recognition over the course of time.

AWS DevOps Guru and Azure AI Insights, for example, have the ability to continuously monitor historical failure trends to improve the AI algorithm over time improving further the predictive RCA capability.

Table 2 Challenges and solution

Challenge	**Solution**
Data Privacy and Security	Implement encryption, secure cloud storage, and regular audits to protect system data.
System Integration	Use API-based AI models and cloud platforms for a phased, seamless RCA transition.
Continuous Learning	Regularly update AI models with new system data to maintain high fault-detection accuracy.

5 Case Studies and Real-world Applications

5.1 Case study 1– RCA Assisted by AI in Cloud Infrastructure Management

One of the worlds largest cloud service providers with operations in over 150 countries adopted AI-driven RCA or Root Cause Analysis which improved system reliability and helped teams troubleshoot issues efficiently. The company struggled to find and remedy failures in their highly distributed cloud infrastructure, resulting in longer time to resolution and higher operational costs. [8]

The company adopted AI-enabled anomaly detection and automated root cause analysis (RCA) tools, using machine learning-based log analytics to find overlap between failure patterns from thousands of virtual machines (VMs) and cloud instances. The Natural Language Processing (NLP) and AI-assisted log parsing capabilities in the solution enable the system to self-identify correlation of error logs, root cause analysis, and take action by generating alerts in a proactive manner. [9]

- Due to this AI-powered RCA solution implementation, the organization announced:
- An average 40% improvement in mean time to resolution (MTTR) of cloud service outages.
- Improved infrastructure reliability of 30% which means more uptime of services.
- A drop of 20% in system outages reported by customers as AI-powered diagnosis uses insights to identify problems and remediate them before impacting them. [10]

Secondly, implementation of AI-assisted RCA, which guarantees the standard protocols and reduces human-error in troubleshooting. This implementation has successfully demonstrated how transformational AI can optimise RCA, improve operational performance, and ensure that cloud computing services are continuously available.

5.2 Case Study 2 – Predictive RCA indistributed data processing systems

A well-known Financial Services Company wanted to improve failure prediction and RCA in its distributed data processing environment, which processed millions of transactions a day across multiple cloud-based data centres. The system's frequent breakdowns caused the firm to experience delays while processing transactions, higher downtime, and disappointed customers. [11]

They used predictive analytics and created machine learning-based RCA to detect issues that would lead to outages allowing them to recover and restore in advance making the systems resilient. Proactively identify potential failures by monitoring various data feeds of historical failure data, log events, and system performance metrics for early warning signals through an AI model. [12]

- Among the important features of predictive RCA system were:
- Patterns of recurring database failures that pattern recognition algorithms used for distributed databases identified.
- Anomaly detection in real-time that sent alerts for data discrepancies and processing bottlenecks.
- Automated remediation workflows that pre-emptively implemented remedies e.g. implementing a auto-scaling of the computational resources during peak-load windows
- As a result of predictive RCA adoption, the company realized:
- 35% Improvement in uptime of systems, leading to greater customer satisfaction
- Reduction of 25% in operating costs due to proactive maintenance enabling less crisis-level troubleshooting costs.
- 50% of faster RCA, with the help of AI-based insights, engineers were able to find the source of the failure faster, and remedial measures were able to take fast action. [13]

The ability to prevent failures, enhance service reliability, and optimize system performance are the major takeaways of this case study highlighting predictive RCA. By moving from solving problems when they arise to preventing failure before it happens, the organization was able to improve operations, reduce downtime and provide uninterrupted service. [14]

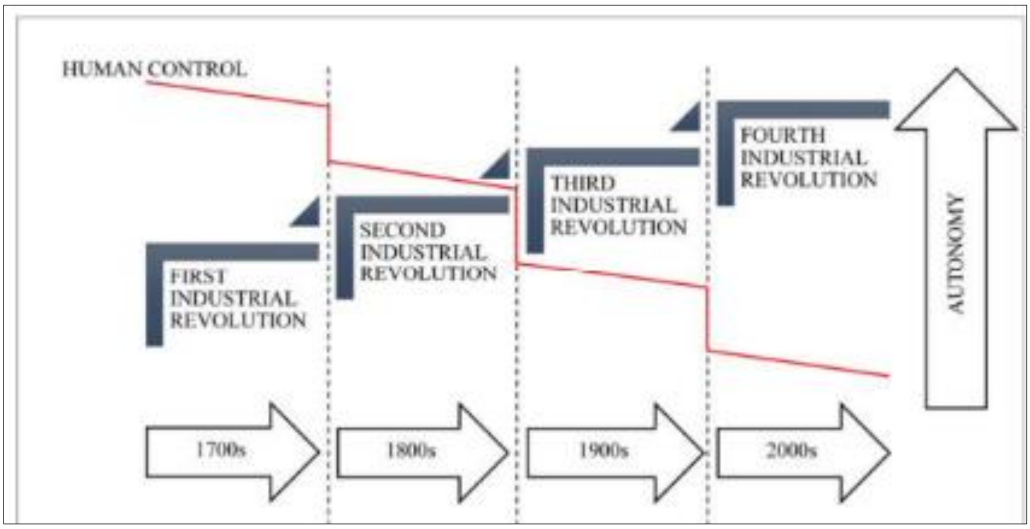
HUMAN CONTROL
FIRST INDUSTRIAL REVOLUTION
SECOND INDUSTRIAL REVOLUTION
THIRD INDUSTRIAL REVOLUTION
FOURTH INDUSTRIAL REVOLUTION
AUTONOMY
1700s
1800s
1900s
2000s

Figure 3 Technology Revolutions Timeline 1 [11]

6 Conclusion

Integrating AI and ML powered Root Cause Analysis (RCA) for Distributed Data Processing Systems comprise a quintessential part of this continuous automation process strengthening operational efficiency, system reliability ensuring proactive troubleshooting. Such automation of repetitive RCA tasks, predictive failure detection and personalization of system diagnostics enhances service availability and performance optimization through these technologies.

Organizations can improve the failure diagnosis process by using AI-driven automation that reduces manual diagnosis and troubleshooting efforts. Automated log analysis and anomaly detection tools powered by AI and machine learning facilitate automated detection and response to system errors, minimizing human error and enforcing a systematic approach to issue resolution. Such automation enables IT teams to concentrate on the complex system failures to which they respond, thus accelerating incident response times while enhancing the resilience of the infrastructure.

Also, instead of being reactive, RCA methodologies are powered by predictive analytics with ML models that helps now in monitoring the system in proactive way. These models study historical system data, identify signs of failure, and prevent these signs from evolving into critical incidents for uninterrupted system functionality. Cloud based AI based monitoring tools can notify administrators of imminent service disruptions and take pre-emptive action to avoid failure from affecting end-users. It improves the dependability of the whole system and increases the confidence of user in distributed computing environment.

In addition to automation and predictive analytics, AI-driven RCA solutions improve system adaptability and customizing capabilities. Constant analysis of historical solutions and practical trends in failures helps AI models to optimize approaches to troubleshooting and offer recommendations that uniquely with the particular architecture and workload of each system. This allows for precise fault diagnostics to be preformed and implemented remediations steps that translates to improved operations and minimized downtime.

However, there are challenges associated with incorporating AI and ML into an RCA capability that must be overcome before adoption in an organization. Privacy and security concerns still loom large, because AI-driven RCA solutions need access to many system logs and performance data. This means that you will need to have data protection compliance with GDPR, CCPA, or the other data compliance legislation as well so that data can be security and trust can be built with the users. Organizations need to ensure strong encryption mechanisms, access control mechanisms, and regular security audits to protect sensitive system information.

The integration of AI-enabled RCA tools with the existing IT infrastructure is another major hurdle to be crossed. A lot of organizations have a hard time integrating AI-based failure diagnostics into their legacy systems causing compatibility issues and service interruptions. A systematic AI implementation approach in multiple phases for instance through API integration and driving cloud deployment can reduce the associated risks, enabling seamless transitions and preventing business disruptions.

Additionally, to keep AI relevant in RCA workflows, there must be continuous learning of the system, and adoption of model retraining. Real-time data and continuous optimization of algorithms are needed as RCA models based on AI depend on ever-changing system architectures and constantly evolving failure patterns. Org need to invest in AI lifecycle management to ensure that AI models are relevant, accurate and efficient in diagnosing complex system failures.

Going forward, AI and ML are going to continue to evolve, continuing to drive RCA functionality while causing the management of distributed data processing to evolve. With other organizations, the same concern with AI-driven RCA solutions, will help them understand the way that own systems can work best and reduce risk of failures & optimize functioning and such organizations will only benefit from edge over others! Overcoming the challenges of data privacy, problems in seamless integration, and the need for continual learning gain enterprises close to the full potential of AI and ML that they can realize through strong, robust, reliable, and intelligent RCA frameworks to drive their long-term digital transformation and innovation.

References

[1] P. W. &. O. K. Thorsten Wittkopp, "LogRCA: Log-Based Root Cause Analysis for Distributed Services," springer, 2024.

[2] A. B. Jacopo Soldani, "Anomaly Detection and Failure Root Cause Analysis in (Micro) Service-Based Cloud Applications: A Survey," acm, 2022.

[3] Y.-K. C. a. C.-P. C. CHI-LU YANG, "AN ANALYSIS OF THE ROOT CAUSES OF DEFECTS INJECTED INTO THE SOFTWARE BY THE SOFTWARE TEAM: AN INDUSTRIAL STUDY OF THE DISTRIBUTED HEALTH-CARE SYSTEM," worldscientific, 2013.

[4] A. Fang, "Root Cause Analysis for Distributed Systems," JOURNAL OF LATEX CLASS , 2015.

[5] R. V. O. V. V. M. L. Timo O.A. Lehtinen, "A tool supporting root cause analysis for synchronous retrospectives in distributed software teams," sciencedirect, 2014.

[6] X. L. ,. Z. H. L. H. Abhishek Jayswal a, "A sustainability root cause analysis methodology and its application," sciencedirect, 2011.

[7] A. M. I. G. Weidl, "Applications of object-oriented Bayesian networks for condition monitoring, root cause analysis and decision support on operation of complex continuous processes," sciencedirect, 2005.

[8] A. H. G. K. Arnak Poghosyan, "Incident Management for Explainable and Automated," Journal of Universal Computer Science, 2021.

[9] A. T. K. P. R. P. Subba Rao Katragadda, "Machine Learning-Enhanced Root Cause Analysis for Rapid Incident Management in High-Complexity Systems," Journal of Science & Technology, 2025.

[10] M. Zasadziński, "Model driven root cause analysis and reliability enhancement for large distributed computing systems," upcommons, 2018.

[11] T. C. Sakuneka, "A Systematic Literature Review of Industry 4.0 Competencies for a Control Systems Engineer," proquest, 2018.

[12] T. V. H. John S. Osmundson, "A Systems Engineering Methodology for Analyzing Systems of Systems," citeseerx, 2020.

[13] A. Gorod, B. Sauser and J. Boardman, "System-of-Systems Engineering Management: A Review of Modern History and a Path Forward," ieeexplore, 2008.

[14] J. S. Osmundson, "A systems engineering methodology for information systems," incose, 2000 .