International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||10||Pages||1647-1657||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i10.ec11

Intelligent Fault Detection and Self-Healing Architectures in Distributed Software Systems for Mission-Critical Applications

Gireesh Kambala
MD, CMS Engineer, Lead, Teach for America, USA.

Abstract-
Self-healing and intelligent fault detection systems are very vital frameworks if we are to raise the dependability and resilience of distributed software systems in mission-critical applications. By use of contemporary technologies including predictive analytics, machine learning, and adaptive algorithms, these systems independently repair errors, actively evaluate system health, and find anomalies: Among the techniques these systems apply to keep low operational costs, continuous service delivery, and little downtime are redundancy, failover systems, and real-time diagnostics. Systems with self-healing capability offer scalability and fault tolerance in both dynamic and demanding environments as well as in optimal performance with various workloads. Using reference to its main features, advantages, and techniques, this book discusses intelligent defect management. The focus is on how these satisfy the dependability standards in domains such aviation, finance, and healthcare. This highlights the possibility to reorganise these systems to enhance operational resilience and efficiency, hence strengthening the dependability and autonomy of dispersed systems.

Keywords: Fault detection, self-healing architectures, distributed systems, mission-critical applications

I. Introduction

The explosive spread of distributed software systems has produced notable developments in vital fields including smart cities, finance, healthcare, and aerospace engineering. Distribution architecture, multi-node interactions, and real-time decision-making requirements define modern technical infrastructure. Their complexity and importance make them prone to flaws like hardware failures, software bugs, network interruptions, and security lapses. Failures in mission-critical distributed systems could cause operational disturbances, financial losses, and maybe jeopardise human life. Consequently, because they provide resilience, adaptation, and autonomy in these situations, intelligent fault detection and self-healing systems have become extremely important in research.

[1]. Machine learning (ML), artificial intelligence (AI), edge computing these systems allow little human intervention proactive detection, analysis, and fault mitigating action. Intelligent fault detection systems find possible faults before they become serious issues using predictive analytics, anomaly detection methods, and real-time monitoring. Among other approaches, deep learning and reinforcement learning have shown to be very useful in enhancing the accuracy and efficiency of defect detection systems thereby enabling systems to identify minor trends suggestive of anomalies. Conversely, self-healing systems on the other hand use autonomous recovery mechanisms including dynamic resource allocation, micro services reconfiguration, and real-time replication of critical components to assure continuation of operations. Including self-healing features into distributed systems lowers mean time to recovery (MTTR), lessens service interruptions, and improves general system dependability. The acceptance of distributed ledger technologies such as

blockchain has helped to build tamper-proof audit trails, so enhancing the traceability and responsibility of fault-management techniques[2]–[4].

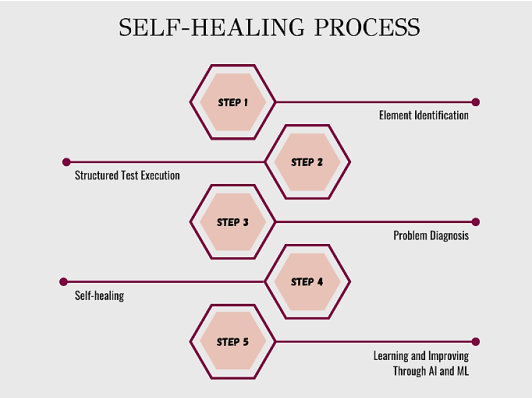

Figure 1 Self-Healing Process [5]

These designs are using federated learning paradigms and edge artificial intelligence more and more as they change to enable distributed fault management at the source, hence lowering latency and improving scalability. Intelligent fault detection and self-healing systems have transforming potential, but they also present difficulties including the significant computational cost, the need of strong cybersecurity protections, and the difficulty of combining several technologies into coherent frameworks. Research is thus focused on optimising these systems by means of creative ideas including hybrid artificial intelligence models, lightweight neural networks, and adaptive feedback loops. Apart from these advancements, Kubernetes' container orchestration features clearly show the value of cloud-native technology[6]–[8]. Maintaining fault tolerance calls for scalability, application of distributed software systems—which these technologies offer, and perfect implementation. By simulating several failure situations and offering perceptive analysis, the availability of digital twins—virtual replicas of real-world systems—helps to increase predictive maintenance capacity. Together, digital twins and intelligent problem detection promise preventive steps guaranteeing operational efficiency or system integrity. Also very important is the focus on cooperative fault control in these systems. Systems can arrange failure detection and recovery activities over several nodes without centralised control by means of distributed artificial intelligence models and distributed consensus protocols. This decentralisation ensures that, even in the case of individual mistakes, the entire system remains robust and functional. More importantly, new ideas in data transfer and interoperability enable to better mix several components, so allowing a more harmonic fault management system[9], [10]. Beyond traditional industries, smart defect detection and self-healing are crucial in creative ones such industrial automation, space exploration, and driverless autos. Self-healing systems' constant reorganising of system settings lowers risks for autonomous cars; for instance, fault detection systems ensure the accuracy of sensor data and decision-making algorithms. Comparably in space exploration, where system failures could have long-lasting effects, comparable ideas boost mission success rates and enable real-time anomaly resolution. Socially speaking, the acceptance of intelligent fault detection and self-healing systems improves sustainability and resource economics. These designs lower the environmental impact of large-scale distributed systems by optimising resource use and lowering of downtimes. Moreover, they improve the dependability and security of vital infrastructure, hence building public confidence in technologically driven solutions. Incorporation of quantum computing, which promises exponential gains in processing capacity, will decide future path of intelligent fault detection and self-healing systems. Quantum algorithms may transform defect detection methods even in very complicated systems by allowing faster and more accurate anomaly analysis. Inspired by the human brain, further expected to guide the building of ultra-efficient and adaptive fault management systems is development in neuromorphic computing[11].

II. Literature Review

Bhide 2025 The advent of sixth-generation (6G) communication systems introduces transformative technologies that surpass previous generations, emphasizing AI integration for intelligent resource allocation and autonomous network management. This review highlights 6G's architecture, featuring terahertz frequencies and integrated satellite networks, poised to redefine connectivity. Key challenges include spectrum scarcity, energy efficiency, and global standardization. Security concerns from expanded attack surfaces are critical. Applications like edge AI, AR, and IoT showcase 6G's potential to revolutionize industries through low latency, high bandwidth, and massive device connectivity[12].

Zhang 2024 Distributed Satellite Information Networks (DSIN) represent a breakthrough in satellite-based communication, addressing challenges in scalability, resource management, and heterogeneity. Integrating clustered satellite systems enables unified data processing across communication, navigation, and remote sensing domains. Innovations such as cloud-native distributed MIMO, grant-free access, and channel modeling improve DSIN's performance. Cross-layer optimization enhances deterministic and adaptive services. Future directions aim at overcoming decentralized frameworks and sparse resources to realize a cohesive, resilient satellite-integrated Internet for next-gen intelligent applications[13].

Trivedi 2024 Industry 5.0 redefines industrial processes by integrating human elements with AI-driven decision-making, enhancing customization, efficiency, and cost reduction. Transparent and interpretable AI models ensure autonomous yet explainable operations, addressing critical downtime issues. Explainable AI (EXAI) facilitates human-machine collaboration, supporting CPSs, smart grids, and digital twins. This review introduces a reference architecture for EXAI in Industry 5.0, with a taxonomy addressing challenges in real-time applications. A manufacturing case study highlights EXAI's transformative role, along with emerging opportunities[14].

Davis 2024 Stress significantly impacts cybersecurity analysts in high-pressure environments, necessitating effective mitigation strategies. This review explores how advancements in IoT and Big Data technologies intersect with human emotions. Stress detection systems leveraging sentiment analysis and e-commerce data aim to enhance productivity by preemptively addressing mental health concerns. Focus areas include understanding how unmanaged stress affects performance and developing tools to alert analysts early. The integration of wearable devices and smart systems underscores the potential for stress management solutions[15].

Moghaddasi 2024 Deep learning (DL) accelerators face critical dependability challenges, particularly from CMOS aging effects, which induce permanent faults and timing errors. This review categorizes resilience strategies for addressing aging in DL systems, emphasizing layer-wise analysis and fault mitigation techniques. Dependability in safety-critical applications like autonomous vehicles remains a key concern. Emerging research directions explore optimal design strategies to maintain efficiency and robustness, ensuring long-term performance in AI-driven systems. This paper offers understanding on how to solve reliability in contemporary DL designs[16].

Table.1 Literature Summary

Authors	Methodology	Research gap	Findings
Pistoia 2023 [17]	Demonstrated an 800 Gbps QKD-secured optical channel with C-band multiplexing over 100 km, integrating	Lack of practical implementations of high-capacity QKD-secured channels for industry use.	Validates QKD-secured channels for metro-scale mission-critical environments like Inter-Data Center

	blockchain for secure transactions.		Interconnects.
Issa 2023 [18]	Explored CE practices in B2B systems at Ericsson, deriving the HURRIER process for improving outcomes.	CE has been widely studied for web-facing applications but not for B2B mission-critical systems, leaving gaps in understanding its application in high-stakes environments	Classified CE practices and demonstrated their value in delivering high-quality B2B solutions.
Paladin 2023 [19]	Explored 5G slicing, low latency, and machine-type communication in MCC scenarios, supported by H2020 RESPOND-A pilots for earthquakes, forest fires, and maritime SAR operations	Limited practical implementations of 5G capabilities in MCC scenarios across diverse environments.	Demonstrated 5G-enabled SAR efficiency through real-world pilots, showcasing improved coordination and timely response for MCC applications.
Duarte 2022 [20]	Developed a fault-injection add-on for a publish/subscribe broker and conducted experiments simulating IoT scenarios with and without self-healing mechanisms.	Lack of systematic evaluation of fault-tolerance mechanisms in mission-critical IoT systems	Fault-injection effectively tests fault-tolerance apparatus, identifies performance lapses, and provides insights for enhancing fault-tolerance in IoT systems
Gutiérrez 2022 [21]	A generative model of cognitive architectures for autonomous robots, integrating cognitive functions and reasoning, following model-	Robots face challenges in ensuring dependability and autonomy due to hardware/software faults and complexity in cognitive integration.	The approach provides a model-based solution for certifiable dependability, enhancing autonomy through formal cognitive integration.

	based engineering principles for dependability.		

III. Adaptive Fault Detection In Distributed Systems

Adaptive fault detection in distributed systems determines the reliability and availability of mission-critical applications. Under such systems, in which numerous components interact via a network, hardware failures, communication interruptions, or software faults can all lead to difficulties. Conventional fault detection methods would not be enough for the dynamic character of distributed events depending usually on predefined thresholds or static error models. Constant learning and adaptation to changing system behaviour help adaptive fault detection systems exceed this limit. Usually detecting unexpected trends in real-time data streams using statistical models or machine learning, these systems modify their detection strategy depending on system status. One of the important characteristics is the ability to distinguish between temporary and permanent flaws since it helps the system to stop ineffective healing systems[22].

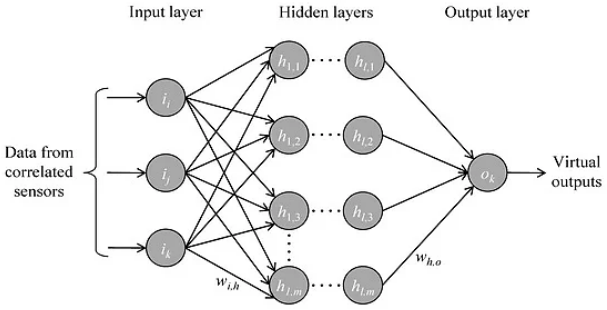

Figure 2 Adaptive Fault Detection in Distributed Systems [23]

Although ongoing issues call for more comprehensive corrective action requiring failover or resource reallocation, local retries could help to manage transient failures. Moreover very important for adaptive fault detection is the use of distributed monitoring agents cooperating to locate and correct flaws across numerous system nodes. These agents guarantee appropriate defect diagnosis by means of information flow and consensus approaches even in cases of individual agent failure. Applied to suitably depict normal system behaviour and point deviations are techniques including probabilistic thinking, time-series analysis, and anomaly detection. Adaptive fault detection offers a proactive means to preserve system integrity in mission-critical systems, where erroneous operations or downtime could have major effects. It lets systems react to novel kinds of difficulties without depending on human reconfiguration or intervention. Adaptive detection systems guarantees that fault tolerance is strong and efficient as systems grow and change, therefore supporting the general dependability of the distributed system. Adaptive fault detection systems especially in dynamic and mission-critical contexts provide several benefits that increase distributed system dependability and efficiency. From these systems, constant learning and adaptation to changing conditions generates more exact and responsive fault identification[24]–[26].

Low false positives, dynamic adaptation, proactive fault management help adaptive systems to quickly find and fix issues, hence minimising disturbance. Large-scale, sophisticated distributed architectures could find fit since they are scalable, efficient, and able of running independently[27]. Adaptive defect detection systems offer the following main benefits:

1. **Dynamic Adaptation:** Adaptive systems increase detection accuracy in dynamic contexts by modifying detection mechanisms depending on real-time fluctuations in system behaviour.

2. **Reduced False Positives:** By distinguishing transitory from permanent issues, adaptive systems save unnecessary recovery efforts and consequently improve general system efficiency.
3. **Scalability:** Large-scale distributed architectures offer effective fault detection over many nodes without sacrificing performance, hence they fit these systems.
4. **Proactive Fault Management:** Early detection of potential issues enabled by adjustable detection speeds helps to lower damage or downtime.
5. **Enhanced Reliability:** The ongoing learning process guarantees great system dependability since the system can adjust to new fault patterns and stop problems before they become more severe.

IV. Self-Healing Architectures For Critical Applications

Self-healing architectures help to ensure the reliability and availability of critical applications, particularly in environments where downtime could have severe consequences. Without human involvement, these systems independently find, diagnose, and fix problems. Using anomaly detection and machine learning models to find deviations from expected behaviour, fault detection is ongoing monitoring of system health using real-time data. When a defect is found, the system starts autonomous recovery activities include rerouting traffic, restarting parts, or reallocating resources to restore capability. Self-healing systems rely on redundancy and failover technologies to make sure backup resources or components may take over effortlessly should a failure occur[28]. Self-optimization and adaptability to changing situations by dynamically altering resource allocation and performance parameters to preserve efficiency and minimise downtime define many designs. By means of constant learning made possible by machine learning, the system can enhance fault identification and recovery techniques grounded on past data. Designed for scalability as well, self-healing systems enable efficient operation in vast, dispersed settings. By lowering manual intervention and automating fault management, self-healing systems increase the availability, dependability, and general performance of significant applications by so making them indispensable for mission-critical operations in sectors including healthcare, finance, aerospace, and telecommunications. Especially in situations when system failure or downtime could have major consequences, self-healing solutions are crucial in ensuring the availability, reliability, and resilience of mission-critical systems[29]. By means of autonomous detection, diagnosis, and fault recovery without human involvement, these systems minimise the effect of faults on system performance. The foundation of self-healing is essentially the capacity of a system to adapt and restore its functioning upon a divergence from its expected behaviour. Healthcare systems, aerospace, defence, telecommunications, and financial services depend on this capacity since continuous functioning is vitally important[30].

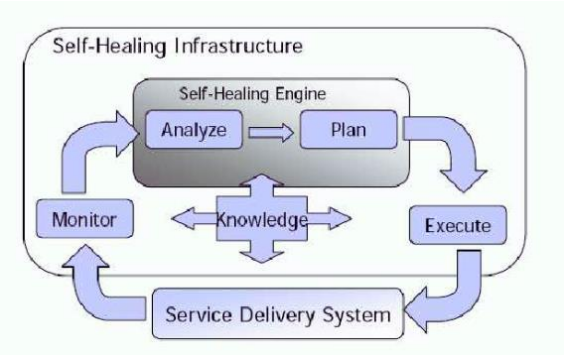

Figure 3 Self-Healing Infrastructure[31]

A. Key Characteristics of Self-Healing Architectures

Some basic properties of self-healing systems are defined by advanced fault detection, autonomous recovery, redundancy mechanisms, self-optimization, and learning capacities. These systems track health in

real-time, diagnose issues, and start recovery activities right away to restore normal operations. They also learn constantly to adapt to new failures, hence ensuring robustness and minimal disturbance[32].

- Fault Detection and Diagnosis: Real-time system state monitoring in modern fault detection systems applied in self-healing systems Both passive and active monitoring methods help these systems find anomalies like hardware faults or performance degradation. Once a problem is found, the system starts diagnostic procedures to identify its degree and cause. Frequently consisting of comparing system logs, performance metrics, and failure trends using machine learning approaches or rule-based systems, this diagnostic stage frequently correct diagnosis of problems ensures suitable methods of system recovery.
- Autonomous Recovery**:** Should a fault be found and recorded, the system starts autonomous recovery. Simple fixes like restarting failing components to more difficult chores like rerouting network traffic, reallocating computing resources, or replacing defective hardware could be part of recovering systems. If a virtual machine breaks without compromising the service, for a cloud-based application, for example, the self-healing mechanism might rapidly move work to a healthy instance. Autonomous recovery seeks to quickly return the system back into normal operating condition, hence lowering service interruptions.
- Redundancy and Failover Mechanisms: Systems of self-healing are essentially based on redundancy. Designed with built-in redundancy—that is, many copies or backup resources—systems can cover should a major resource fail. A distributed database system consists in many replicas of data split over several nodes; should one node die, data availability is changed. Failover systems allow a broken component quick transition to its backup, therefore guaranteeing ongoing service delivery with minimum disturbance.
- Self-Optimization**:** Self-healing systems often include self-optimizing elements in addition to fault detection and recovery. These devices track performance criteria constantly and modify their behaviour or configuration to maximise the available current resources. Dynamic resource scaling based on traffic load or energy consumption improves fault tolerance and increases general efficiency in a self-healing architecture in a cloud application. Self-optimization guarantees that the system not only solves problems but also adjusts to changing environments, so maintaining perfect performance throughout time.
- Learning and Adaptation: Many self-healing systems offer ongoing learning and adaptability by including machine learning, artificial intelligence, and other approaches. Previous performance allows the system to evaluate past failure records & modify its fault detecting & recovery strategies. This learning method helps the system to predict any issues before they start and regulates several forms of mistakes. By use of predictive analytics, the system may forecast failures based on trends, therefore offering early warning and facilitating proactive recovery projects[33].

B. Advantages Of Self-Healing Architectures

Especially in terms of improving the economy of relevance and performance of important applications, self-healing methods present tremendous benefits. These systems automated diagnosis, problem identification, and recovery techniques offers amazing availability and thereby lowers downtime. This clarifies users' experience. Reducing the need for human interaction also helps to decrease running expenses, therefore allowing effective use of resources. Self-healing systems also improve system reliability and allow to stay functioning even during breakdowns by means of constant monitoring and quick problem solving. Their scalability promotes growth and helps one to be used conveniently at many scattered locations without sacrificing performance[34].

- Increased System Availability**:** Self-healing systems guarantee amazing availability even in the situation of a breakdown by automating fault detection, diagnosis, and recovery, so ensuring that vital

applications stay available. Systems improve user experience and help to reduce downtime by tackling problems free of human participation.

- Reduced Operational Costs: Self-healing technology let companies better manage resources by lowering the need for human monitoring and intervention. Automation of recovery systems especially in mission-critical events helps to lower related system breakdown costs.
- Enhanced Reliability**:** Fast fault discovery and rectification made Guarantees system reliability come from self-healing systems. Automated reflexes and constant monitoring guarantee that systems remain operational even in the situation of particular component failure.
- Scalability: Large, distributed cases whereby hand error detection and recovery would not be viable for these scalable systems. Self-healing systems can grow to provide new components and services without sacrificing performance as applications get more sophisticated[35].

V. Reliability Through Intelligent Fault Management

Good systems are predicated on dependability; thus, even little adjustments can have a big impact. Better detection, diagnosis, and recovery methods guaranteed by intelligent fault management—a logical process—ensures ongoing system reliability. This method automatically finds and fixes errors with modern technologies including artificial intelligence, machine learning, and real-time analytics, therefore lowering the risk of system failure and outage[36].

- **Advanced Fault Detection:** Intelligent fault management makes advantage of advanced detection techniques capable of continuous monitoring of system state. These systems search system logs, performance criteria, and communication patterns for variations signalling possible problems. Intelligent systems actively adapt to changing situations, unlike fixed-threshold based conventional methods, therefore increasing their capacity to identify both temporary and chronic flaws. This proactive detection tool maintains system integrity and user delight by means of ensuring that issues are resolved before they become more critical.
- **Accurate Fault Diagnosis:** Once an issue is discovered, the fundamental reason must be identified with a proper diagnostic. Intelligence systems link data from many sources—hardware metrics, software logs, network activity—using computer learning models and rule-based approaches. These systems separate hardware failures, software problems, and outside disturbances thereby allowing targeted recovery actions. AI-driven analytics helps to lower false positives and speed responses, thereby allowing ongoing progress in diagnosis accuracy.
- **Autonomous Recovery Mechanisms:** Smart fault management systems are supposed to start their own healing process. These tasks can cover everything from reallocating resources to perhaps generating failover to duplicate systems to restarting a broken component. Fast and constant recuperation enables automaton to cut running costs and human interaction. Regarding cloud solutions, workloads can be easily moved to healthy nodes without end user compromise, so preserving excellent availability.
- **Predictive Analytics for Fault Prevention:** Predictive analytics uses trend analysis and prior data to foresee probable issues, therefore adding even more reliability. By use of pattern recognition connected with past mistakes, the system may proactively address vulnerabilities before they generate outage. Predictive maintenance methods extend the running lifetime and improve the general resilience of the system by substituting hardware approaching its failure threshold.
- **Scalability and Adaptability:** Naturally scalable and suited for complex, scattered situations, intelligent fault management solutions Their learning characteristics adapt to match the growing complexity of contemporary systems by changing with changing responsibilities and configurations. This adaptability guarantees continuous dependability as systems get more complicated and vast[37].

VI. Conclusion

Particularly for mission-critical applications, distributed software systems depend on intelligent defect detection and self-healing systems absolutely to be dependable, scalable, and resilient. To satisfy the demands of dynamic and complex environments, these designs use modern technologies including autonomous recovery, predictive analytics, and machine learning. By means of a continuous monitoring of system health, anomaly detection, problem diagnosis, and recovery action implementation, these systems minimise running costs, increase performance, and limit outage. Thus, the combination of adaptive mechanisms and self-optimization maintains defect tolerance and efficiency, so enabling systems to fit to the workload and configuration. Moreover ensuring ongoing service availability in the event of failures include cooperative fault diagnostics, failover mechanisms, and redundancy. Since they enable systems of various scope and complexity to be absolutely necessary by way of their flexibility and scalability, these designs are basic in current distributed systems. While intelligent designs provide a proactive, automatic, and robust way of maintaining system integrity, conventional fault management techniques typically fail in dynamic systems. Emphasising their relevance in allowing the operational requirements of mission-critical applications in industries including aerospace, finance, and healthcare, this analysis stresses the need of intelligent fault detection and self-healing in increasing the dependability of distributed systems.

References

1. N. D. Huynh *et al.*, "Adversarial Attacks on Speech Recognition Systems for Mission-Critical Applications: A Survey," 2022, [Online]. Available: http://arxiv.org/abs/2202.10594
2. A. A. Kane, A. G. Marino, F. Fons, S. Nueesch, P. Serwa, and M. Schoetz, "Elastic Gateway Functional Safety Architecture and Deployment: A Case Study," *IEEE Access*, vol. 10, no. September, pp. 91771–91801, 2022, doi: 10.1109/ACCESS.2022.3199356.
3. U. Sikandar *et al.*, "A context-aware and intelligent framework for the secure mission critical systems," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, pp. 1–17, 2022, doi: 10.1002/ett.3954.
4. A. U. Rehman, R. L. Aguiar, and J. P. Barraca, "Fault-Tolerance in the Scope of Cloud Computing," *IEEE Access*, vol. 10, pp. 63422–63441, 2022, doi: 10.1109/ACCESS.2022.3182211.
5. G. Pedrini, "Alma Mater Studiorum Università di Bologna Archivio istituzionale della ricerca Rights / License : The terms and conditions for the reuse of this version of the manuscript are specified in the," vol. 3, no. April 2024, pp. 109–114, 2022.
6. S. Bharany *et al.*, "Energy efficient fault tolerance techniques in green cloud computing: A systematic survey and taxonomy," *Sustain. Energy Technol. Assessments*, vol. 53, 2022, doi: 10.1016/j.seta.2022.102613.
7. C. Nam, S. Math, P. Tam, and S. Kim, "Intelligent Resource Allocations for Software-Defined Mission-Critical IoT Services," *Comput. Mater. Contin.*, vol. 73, no. 2, pp. 4087–4102, 2022, doi: 10.32604/cmc.2022.030575.
8. J. Porter, D. A. Menascé, and H. Gomaa, "A decentralized approach for discovering runtime software architectural models of distributed software systems," *Inf. Softw. Technol.*, vol. 131, pp. 1–50, 2021, doi: 10.1016/j.infsof.2020.106476.
9. M. J. Farooq and Q. Zhu, "QoE Based Revenue Maximizing Dynamic Resource Allocation and Pricing for Fog-Enabled Mission-Critical IoT Applications," *IEEE Trans. Mob. Comput.*, vol. 20, no. 12, pp. 3395–3408, 2021, doi: 10.1109/TMC.2020.2999895.
10. C. Arendt, M. Patchou, S. Bocker, J. Tiemann, and C. Wietfeld, "Pushing the Limits: Resilience Testing for Mission-Critical Machine-Type Communication," *IEEE Veh. Technol. Conf.*, vol. 2021-September, 2021, doi: 10.1109/VTC2021-Fall52928.2021.9625209.
11. H. Farag, M. Gidlund, and C. Stefanovic, "A Deep Reinforcement Learning Approach for Improving Age of Information in Mission-Critical IoT," *2021 IEEE Glob. Conf. Artif. Intell. Internet Things, GCAIoT 2021*, pp. 14–18, 2021, doi: 10.1109/GCAIoT53516.2021.9692982.
12. P. Bhide, D. Shetty, and S. Mikkili, "Review on 6G communication and its architecture, technologies included, challenges, security challenges and requirements, applications, with respect to AI domain," *IET Quantum Commun.*, no. August, pp. 1–23, 2025, doi: 10.1049/qtc2.12114.

13. Q. Zhang *et al.*, "Distributed satellite information networks: Architecture, enabling technologies, and trends," pp. 1–69, 2024, [Online]. Available: http://arxiv.org/abs/2412.12587
14. C. Trivedi *et al.*, "Explainable AI for Industry 5.0: Vision, Architecture, and Potential Directions," *IEEE Open J. Ind. Appl.*, vol. 5, no. July 2023, pp. 177–208, 2024, doi: 10.1109/OJIA.2024.3399057.
15. T. Davis-stewart, "Stress Detection : Stress Detection Framework for Mission-Critical Application : Addressing Cybersecurity Analysts Using Facial Expression Recognition," vol. 2, no. 3, pp. 1–12, 2024.
16. I. Moghaddasi, S. Gorgin, and J. A. Lee, "Dependable DNN Accelerator for Safety-Critical Systems: A Review on the Aging Perspective," *IEEE Access*, vol. 11, no. July, pp. 89803–89834, 2023, doi: 10.1109/ACCESS.2023.3300376.
17. M. Pistoia *et al.*, "Paving the way toward 800 Gbps quantum-secured optical channel deployment in mission-critical environments," *Quantum Sci. Technol.*, vol. 8, no. 3, 2023, doi: 10.1088/2058-9565/acd1a8.
18. D. Issa Mattos, A. Dakkak, J. Bosch, and H. H. Olsson, "The HURRIER process for experimentation in business-to-business mission-critical systems," *J. Softw. Evol. Process*, vol. 35, no. 5, pp. 1–24, 2023, doi: 10.1002/smr.2390.
19. Z. Paladin, E. Kočan, Ž. Lukšić, N. Kapidani, M. A. Kourtis, and M. C. Batistatos, "5G for Mission Critical Communications: RESPOND-A Project Experiences," *2023 22nd Int. Symp. INFOTEH-JAHORINA, INFOTEH 2023*, no. March, 2023, doi: 10.1109/INFOTEH57020.2023.10094163.
20. M. Duarte, J. P. Dias, H. S. Ferreira, and A. Restivo, "Evaluation of IoT Self-healing Mechanisms using Fault-Injection in Message Brokers," *Proc. - 4th Int. Work. Softw. Eng. Res. Pract. IoT, SERP4IoT 2022*, pp. 9–16, 2022, doi: 10.1145/3528227.3528567.
21. S. M. Gutiérrez and G. Steinbauer-Wagner, "The Need for a Meta-Architecture for Robot Autonomy," *Electron. Proc. Theor. Comput. Sci. EPTCS*, vol. 362, pp. 81–97, 2022, doi: 10.4204/EPTCS.362.9.
22. M. Barrère and C. Hankin, "Analysing Mission-critical Cyber-physical Systems with AND/OR Graphs and MaxSAT," *ACM Trans. Cyber-Physical Syst.*, vol. 5, no. 3, 2021, doi: 10.1145/3451169.
23. X. Guo *et al.*, "Towards scalable, secure, and smart mission-critical IoT systems: review and vision," *Proc. - 2021 Int. Conf. Embed. Software, EMSOFT 2021*, pp. 1–10, 2021, doi: 10.1145/3477244.3477624.
24. M. Silva, J. P. Dias, A. Restivo, and H. S. Ferreira, "A Review on Visual Programming for Distributed Computation in IoT," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12745 LNCS, pp. 443–457, 2021, doi: 10.1007/978-3-030-77970-2_34.
25. L. Rosa, W. Song, L. Foschini, A. Corradi, and K. Birman, "DerechoDDS: Strongly Consistent Data Distribution for Mission-Critical Applications," *Proc. - IEEE Mil. Commun. Conf. MILCOM*, vol. 2021-November, pp. 684–689, 2021, doi: 10.1109/MILCOM52596.2021.9653032.
26. S. Lins *et al.*, "Artificial intelligence for enhanced mobility and 5g connectivity in UAV-Based critical missions," *IEEE Access*, vol. 9, pp. 111792–111801, 2021, doi: 10.1109/ACCESS.2021.3103041.
27. D. Yu, W. Li, H. Xu, and L. Zhang, "Low Reliable and Low Latency Communications for Mission Critical Distributed Industrial Internet of Things," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 313–317, 2021, doi: 10.1109/LCOMM.2020.3021367.
28. D. Sobhy, R. Bahsoon, L. Minku, and R. Kazman, "Evaluation of Software Architectures under Uncertainty: A Systematic Literature Review," *ACM Trans. Softw. Eng. Methodol.*, vol. 30, no. 4, 2021, doi: 10.1145/3464305.
29. M. Ndiaye, G. P. Hancke, A. M. Abu-Mahfouz, and H. Zhang, "Software-defined power grids: A survey on opportunities and taxonomy for microgrids," *IEEE Access*, vol. 9, pp. 98973–98991, 2021, doi: 10.1109/ACCESS.2021.3095317.
30. F. Aminifar, F. Rahmatian, and M. Shahidehpour, "State-of-the-Art in Synchrophasor Measurement Technology Applications in Distribution Networks and Microgrids," *IEEE Access*, vol. 9, pp. 153875–153892, 2021, doi: 10.1109/ACCESS.2021.3127915.
31. "Decentralised Control for Distributed Self-adaptive Systems with Strict Quality-of-Service

Requirements," 2021.
32. S. S. Khan and H. Wen, "A Comprehensive Review of Fault Diagnosis and Tolerant Control in DC-DC Converters for DC Microgrids," *IEEE Access*, vol. 9, pp. 80100–80127, 2021, doi: 10.1109/ACCESS.2021.3083721.
33. S. Das, S. Wedaj, K. Paul, U. Bellur, and V. J. Ribeiro, "Airmed: Efficient Self-Healing Network of Low-End Devices," 2020, [Online]. Available: http://arxiv.org/abs/2004.12442
34. D. R. Perez, M. E. Domingo, I. P. Llopis, and F. J. Carvajal Rodrigo, "System and architecture of an adapted situation awareness tool for first responders," *Proc. Int. ISCRAM Conf.*, vol. 2020-May, no. May, pp. 928–936, 2020.
35. N. Burow, R. Burrow, R. Khazan, H. Shrobe, and B. C. Ward, "Moving Target Defense Considerations in Real-Time Safety-and Mission-Critical Systems," *MTD 2020 - Proc. 7th ACM Work. Mov. Target Def.*, pp. 81–89, 2020, doi: 10.1145/3411496.3421224.
36. J. P. Dias, T. B. Sousa, A. Restivo, and H. S. Ferreira, "A Pattern-Language for Self-Healing Internet-of-Things Systems," *ACM Int. Conf. Proceeding Ser.*, 2020, doi: 10.1145/3424771.3424804.
37. S. Paul, F. Kopsaftopoulos, S. Patterson, and C. A. Varela, "Dynamic Data-Driven Formal Progress Envelopes for Distributed Algorithms," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12312 LNCS, pp. 245–252, 2020, doi: 10.1007/978-3-030-61725-7_29.

.