P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

Decentralized Swarm Intelligence for Critical Infrastructure Fault Tolerance

Alexander Miller
Asst Professor

Abstract: Financial systems are becoming increasingly decentralized, comprising distributed nodes that interact fluidly with customers, suppliers, regulators, and other counterparties. These nodes must routinely make fast decisions, and growing evidence shows that the absence of decisions that are both fast and auditable exposes financial institutions to regulatory and reputational risk.

This work addresses that gap by examining evidence-based mechanisms, formal structures, and governance models that enable rapid, auditable decision-making across a wide range of financial systems—from payment rails to multi-institutional settlement waterfalls. We introduce the **decision fabric**, a conceptually simple architecture consisting of layered abstractions with explicit contracts between adjacent layers. Decision fabrics are built on three core principles: distributed provenance capture, distributed operational risk-control governance, and decision governance. Because it is layer-based, a decision fabric can be embedded into any system or application that requires auditable decision-making.

Keywords :Distributed Multi-Agent Systems,Industrial Infrastructure Resilience,Intelligent Agent Coordination,Cyber-Physical Systems,Industrial Internet of Things (IIoT),Distributed Artificial Intelligence,Autonomous Decision-Making,Fault Detection and Recovery,Edge Intelligence,Resilient Industrial Automation

1. Introduction

Distributed multi-agent systems strengthen the resilience of large-scale industrial infrastructure by exploiting coordination, autonomy, scalability, and robustness. By mapping system properties to resilience goals—availability, integrity, continuity, and adaptability—and by making corresponding assessments in industrial settings, suitability is evidenced. Resilience is supported through the combination of theories on multi-agent coordination, capacity for autonomous behavior, and willingness to engage in risk-prone actions. Specific case studies that employ agent-based modeling with distributed planning, decision making, and control are examined.

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

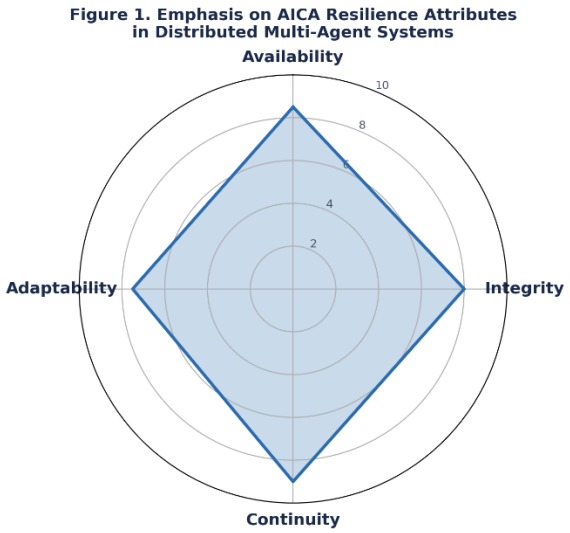


Figure 1. Emphasis on AICA Resilience Attributes in Distributed Multi-Agent Systems

Fig 1: **AICA Resilience Framework** – radar chart of Availability, Integrity, Continuity, Adaptability

Industrial resilience has three views: (1) availability and integrity of the service produced, (2) sufficient redundancy to ensure continuity of operations despite faults and attacks, and (3) adaptability to overcome a disaster by an effectual restoration of the service site. The threat landscape and its risk sources are characterized, and risk likelihood and impact outlined, together with supportive quantitative and qualitative metrics. Requirements for continuity of operations are stated, including the time during which tasks are guaranteed to be performed despite disruption, the framework within which redundancy strategies are decided, and the acceptable time by which a degraded site should recover its intended service use. The potential for resilience is examined by considering a specific case where the service is an automated supply chain.

Resilience Score

$$R_s = \alpha A + \beta I + \gamma C + \delta D$$

Where:
A= Availability, I= Integrity, C= Continuity, D= Adaptability.

2. Theoretical Foundations of Distributed Multi-Agent Systems

The operation of Distributed Multi-Agent Systems (dMAS) appears to be based on four intertwined aspects, namely: foundational theories underpinning the behavior of dMAS, Agent-Based Modeling (ABM), Coordination Protocols and Mechanisms, Emergent Artificial Intelligence (AI). Together, these aspects provide the theoretical basis and practical know-how to specify the required properties of dMAS in general, and their relation to industrial infrastructure resilience in particular.

Availability

$$A = \frac{T_u}{T_u + T_d}$$

Where:
T_u= Uptime, T_d= Downtime.

Fundamental theories underpinning dMAS are rooted in Charles Taylor's (1968) thoughts on the social sciences, naturally adapted to non-human systems and partially reconciled with the current studies in complex systems, and evolutionary theories. Industrial infrastructures consist of many similar interacting parts at different levels of organization, and the key properties of such systems can be derived by using the set of fundamental properties stated for dMAS. Taylor's ideas complement the empirical results obtained for industrial infrastructures, clarify the role of dMAS in the context of modern AI technologies, and support the application of dMAS in social sciences.

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

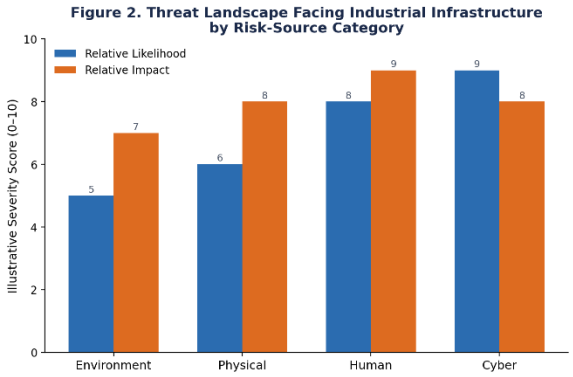


Fig 2: **Threat Landscape by Risk Source** – Environment, Physical, Human, Cyber (likelihood vs. impact)

A. Agent-Based Modeling and Coordination

Coordination is key to the robustness and efficiency of a multi-agent system, spanning shared information, collaborative control, joint execution, and consensus-based problem-solving. Multi-agent systems release global control by distributing low-level decision-making, realizing scalability and fault tolerance. Coordination ensures that individual choices align with over-arching goals, avoiding convergent motion without integration. Multi-agent systems for industrial infrastructure continuously support the AUTOMATION continuum, spreading responsibilities from edge devices to system servers that support, rather than control, operation, maintenance, and recovery.

For addressing operational challenges, data from the network's comprehensive surveillance layer anticipate needs in a timely manner, enabling out-of-band scheduled interventions; higher-level sensors and resources operate under event-driven control; and maintenance, policing, and recovery activities are organized by joint execution and consensus protocols. Dynamic reallocation discovers groups forming and dissolving by necessity rather than by explicit planning, adapting continuously to changing conditions. Continuous availability and reliable integrity should remain under normal conditions, while continuity of operations, practicability of recovery plans, and opportunistic redundancy offset vulnerabilities in those dimensions.

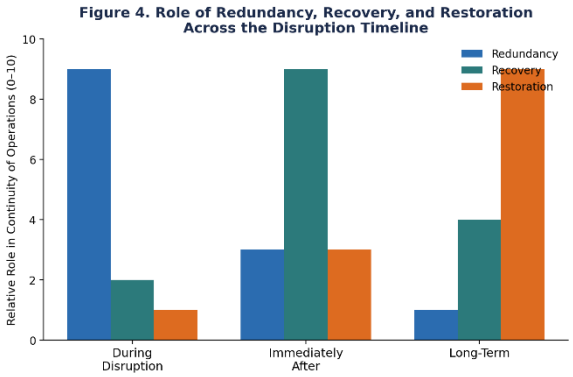
Risk Value

$$R = P_t \times I_t$$

Where:
P_t= Threat probability, I_t= Threat impact.

3. Industrial Infrastructure Resilience: Concepts and Requirements

Research on industrial infrastructure resilience has framed the subject using concepts like availability, integrity, continuity, and adaptability (AICA). These notions cover basic operational capabilities, desired behavior for load transfer on failure, preparatory redundancy measures, and long-term adjustments. Related requirements address indicators (metrics governing the choice of algorithm or method), the threat landscape (risk sources, likelihood, impact), continuity of operations (performance during disruption), recovery properties, and time and cost considerations.



P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

Fig 3: **Layered dMAS Architecture** – Edge → Communication → Coordination → Central Server layers

Industrial infrastructure is a class of critical system that includes power, telecommunications, transportation, finance, liquid fuel, and gas networks. These systems typically exhibit large size and complexity, service a wide variety of users that require different qualities of service, and provide a mix of commercial, public, and end-consumer services. Resilience implies added external and internal robustness against risks from hostile human behavior and system faults. Greed and negligence of employees, criminals making a profit, terrorists aiming at disruption, hackers looking for notoriety, industrial espionage, dishonest competitors, and unfriendly nations all represent real and substantial threats. Efforts to understand the relevant threat landscape have produced extensive catalogs and studies, and consensus has emerged that malicious humans can inflict deliberate, intelligent, and unpredictable damage. Thus, catastrophic failures resulting from attacks can be both complex and costly to mitigate.

Redundancy Factor

$$RF = \frac{N_b}{N_a}$$

Where:
N_b= Backup nodes, N_a= Active nodes.

A. Threat Landscape and Risk Assessment

Industrial infrastructures face a range of potential threats, including natural phenomena, act of God, accidents, human errors, malicious acts, and systemic failures. Risk sources can be classified into four categories: a) environment, b) physical, c) human, and d) cyber. The likelihood of future disruptive incidents can be assessed based on historic data, examination of past incidents and near-miss cases, and statistical studies. A combination of quantitative and qualitative methods, the latter relying on expert judgments, can be used to determine the impact of potential disruptive incidents on the required continuity of operations and service.

Table 1. Core Resilience Attributes

Attribute	Meaning	Role in Industrial Infrastructure
Availability	Service remains accessible	Maintains operation during normal and stressed conditions
Integrity	Data and control remain reliable	Prevents corrupted or false information
Continuity	Service continues during disruption	Supports critical functions during failures
Adaptability	System adjusts after disruption	Enables recovery and restoration

Continuity of operations refers to the capability of an organization to continue to perform its essential functions during a disruption, be it natural or human-induced; this concept links to the analysis of prospective risk. The three classes of continuity strategies are redundancy, recovery, and restoration. Redundancy allows maintaining the same level of service during a disruptive incident by switching to an unexpected or less preferred functioning mode. Recovery refers to the planned resumption of proper operations after the incident has passed; recovery-related objectives specify the parts of the system that must be restored by the business after a disruptive event. Restoration means the capability to return to normal operations at some point after the incident. Finally, the required degree of resilience encompasses all five preceding principles and reflects the level of service provision during disruption.

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

Fault Tolerance Index

$$FTI = \frac{N_s}{N_t}$$

Where:
N_s= Surviving agents, N_t= Total agents.

B. Continuity of Operations and Redundancy

Continuity of operations is a core goal in resilience-building strategy, defined here as the ability to continue providing critical services and functions before, during and after disruptive events. Redundancy is a commonly adopted strategy for enhancing continuity of operations, in which backup or excess capabilities are employed to absorb the effects of disruptive events. This redundancy may manifest in many forms, such as alternative pathways in transportation networks and alternative sources of power for critical facilities. Historical records of catastrophic failure offer one way to determine the redundancy levels required for continuity of operations. In addition, redundancy levels can be set to achieve defined recovery objectives, such as restoring a transport network within a predefined number of hours after a flooding event.

Table 2. Multi-Agent System Features

Feature	Description	Resilience Benefit
Coordination	Agents share information and actions	Improves collective decision-making
Autonomy	Agents act independently	Reduces dependence on central control
Scalability	System grows across many assets	Supports large industrial networks
Robustness	System tolerates faults and attacks	Prevents complete service failure

Continuity of operations can also be ensured through the application of redundant control schemes that govern the operation of a civil infrastructure system. Redundant control schemes facilitate rapid control system reconfiguration following a disruption.

4. Architecture of Distributed Multi-Agent Solutions

Solutions based on distributed multi-agent systems (MAS) should be tailored for the addressed context in order to be effective. Design decisions take into account critical attributes of the context while maintaining a general CSI orientation. The main features of the involved architecture, inspired by the considerations presented above, comprise layered implementation, a set of defined interfaces, and support for interoperability among solutions developed by different organizations. Fundamental aspects of the system architecture are discussed, focusing on the roles of agents, central servers for specific tasks (when needed), and edge components with more limited resources located close to the physical assets of the critical system, responsible for data gathering and some decision-making.

Consensus Decision

$$D_c = \frac{1}{n}\sum_{i=1}^{n} d_i$$

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

Where:
d_i= Decision of agent i, n= Number of agents

Emergent properties of multi-agent systems are largely determined by how they control their interactions and information exchanges. For situational awareness and other functionalities requiring information from multiple agents, these capabilities can be implemented in central servers. However, such servers should be designed to avoid becoming scalable bottlenecks and single points of failure. Data fusion and the integration of information from multiple heterogeneous sensors are key challenges. State estimation is fundamental for continuity of operations, and its quality directly influences the overall level of safety and security of the critical system. Situational awareness possesses a primary role in risk assessment, being modeled as a consistency check on the information flowing through the system.

A. System Architecture and Layering

The architecture of distributed multi-agent solutions in industrial contexts emphasizes practical design while avoiding excessive detail. The system comprises multi-agent solutions and other solutions hosted on central servers and edge components. Multi-agent solutions typically reside on the central servers. They are composed of multiple agents defined in a shared communication environment, allowing them to communicate with one another and support any application that requires information fusion, data transfer, or distributed decision-making. Applications for edge components are hosted on two dedicated open-source software applications. Edge components and the central servers can be operated independently or together. The edge components provide interfaces to industry-specific data sources and act as multi-agent nodes processing distributed elastic data. Alternatively, multiple edge components connect to a central server that aggregates their data, applying any multi-agent solution that cannot be hosted at the edge layer.

Seamless data and information sharing across all components is essential. Four data fusion, sensor management, state estimation, and situation-awareness functions address this need. Data fusion answers requests for critical information needed by modules and agents across the system. Sensor management ensures that the effect of faults and attacks on the sensors is minimized. State estimation prepares local state-estimation requests into a centralized task, allowing each participating edge component to contribute by monitoring the part of the system within its own local horizon. Situation awareness responds to information requests related to different domains, such as enemy activity, environmental conditions, and the physiological and emotional state of human agents, by fusing relevant information from the contributing nodes.

Table 3. Industrial Threat Categories

Threat Category	Examples	Possible Impact
Environmental	Flood, fog, snow, disaster	Service interruption
Physical	Equipment failure, asset damage	Operational breakdown
Human	Error, negligence, malicious acts	Safety and reliability risks
Cyber	Hacking, message corruption	Control and data compromise

B. Data Fusion and Situation Awareness

A distributed hazard monitoring and forecasting system involves a multitude of sensors distributed over a wide area, detecting local hazard conditions, relaying them to nearby edge nodes, and facilitating localized hazard warnings. Such a system lays the foundation for the situation-awareness layer and global hazard model across the agent-based system.

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

Data Fusion Output

$$F_d = \sum_{i=1}^{n} w_i \, x_i$$

Where:
x_i= Sensor input, w_i= Weight of sensor i.

A common requirement for large-scale multi-sensor systems is the fusion of data streams at designated aggregation points. Some aggregate the sensor data into joint hazard state estimations, while others retrieve local-data streams from all adjacent neighbor sensors to identify possible anomalous sensor behaviors. The information of different sensors is combined so the situation-awareness layer can assess the hazard situation around its edge node location. It is also possible to apply new detected hazards to a local hazard model among neighboring agents to enhance prediction accuracy.

Communication Reliability

$$CR = 1 - \frac{M_l}{M_t}$$

Where:
M_l= Lost messages, M_t= Total messages

Consideration should also be given to the integration of data from heterogeneous sensor sources. For example, social media user-generated content can be fused with the data from government-maintained embedded hazard monitoring systems to provide information about fog and heavy snow. The situation-awareness functionalities evolve over time since past information can be utilized by agents to learn historical regional hazard patterns and apply ensemble learning to enhance the performance of the region model. Such an online machine-learning approach makes a distributed system more scalable by requiring fewer training samples when dealing with localized hazardous events.

C. Distributed Decision-Making Mechanisms

A variety of distributed decision-making mechanisms have been explored and documented within the context of distributed multi-agent systems. Agencies have been designed to facilitate distributed consensus, conduct dynamic auctions, support event-triggered control actions, handle priorities among teams, and resolve conflicts between agents or teams. These mechanisms can be employed either separately or in combination, adapting to the specific needs at hand.

Consensual decisions are particularly critical during the sensing and situation-awareness phases, where formalized agreements on the interpretation of real-time observations are crucial. Consensus mechanisms have been designed for sampling applications with communication constraints, and experimental results highlight the benefits of group formation, efficiently managing both reliability and bandwidth. In the context of distributed auctioning, agents place offers corresponding to the information they can provide in response to an event, with the best offer ultimately accepted according to a pre-established auction protocol.

Recovery Efficiency

$$RE = \frac{S_r}{T_r}$$

Where:
S_r= Restored service level, T_r= Recovery time.

In team-based solutions, agents may have competing objectives that need to be addressed. To manage such scenarios, priority information has been incorporated into distributed optimal control problems, allowing for prioritized control of multi-agent systems. Priority-based

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

optimal solutions reduce overall cost by transferring allocation responsibility from low-cost agents to those with greater capacity, while guaranteeing satisfaction of all team members. Mechanisms that account for conflicting interests among agents or groups have likewise been considered: a fuzzy-clustering formulation enables distributed suboptimal control of heterogeneous cooperative multi-agent systems, while dissipative dynamic games provide a means for conflict resolution.

Table 4. Continuity Strategies

Strategy	Purpose	Example
Redundancy	Maintain service using backup capacity	Alternative power or network path
Recovery	Resume proper operations	Planned post-incident restoration
Restoration	Return to normal service	Full system recovery after disruption

5. Methods for Ensuring Robustness and Reliability

Fault-tolerance mechanisms enhancing the robustness and reliability of distributed multi-agent systems protect against communication network faults and malicious/accidental attacks by enabling graceful performance degradation in the face of selected failures. Maintaining the availability of components and communication paths increases trust and willingness to use the system, mitigating single points of failure. Fault-tolerance measures extend to communication protocols, preventing cascading network failures; measures against loss of message integrity, latency, or ordering further support reliable communications.

Graceful Degradation

$$GD = \frac{P_d}{P_n}$$

Where:
P_d= Degraded performance, P_n= Normal performance.

6. Conclusion

The presented analysis demonstrates that distributed multi-agent systems are suitable for enhancing the resilience of large-scale industrial infrastructure. The resilience of such infrastructure comprises four attributes: availability, integrity, continuity, and adaptability. A detailed breakdown of each attribute identifies a corresponding set of requirements. Distributed multi-agent systems realize the identified requirements through key properties, among which support for coordination, autonomy, scalability, and robustness are essential. Coordination requirements depend on the particular context and involved agents; when enabled by coordination protocols, these requirements can often be satisfied without complex and computationally expensive optimization. The threat model in industrial settings is larger than in most other applications. Factors capable of imposing affect or disrupting operation stem from both the environment and the human factor. In most cases, risk sources can be classified in terms of likelihood and potential severity. Industrial continuity of operation is defined as a specific minimum level of performance. This minimum performance can be satisfied even under disruption by means of redundancy at different levels—equipment, routing, or functionality. Related redundancy strategies can also be extended beyond the core level of a particular system or service. Essential redundancy can be guaranteed by the inherent properties of the distributed and multi-agent nature of the solution.

The diverse set of threats and related risks mandates a continuity of operation that goes beyond normal availability

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

levels. In extreme cases, the objective may be complete recovery in terms of performance. Euskaltren, the railway company of the Basque government, constitutes a suitable experimental test case for the analysis of distributed multi-agent solutions. Present results concern available designs in optimized consistency control for the specification of role priority in decision controls. Practical implementations of the proposed distributed multi-agent concepts must be validated in other areas of application. The effort should assess the various levels of adaptability, including the possibility of the emergence of pre-specified new functionalities. Finally, new possibilities for policy or standard setting also emerge from the analysis. In such a manner, the previous effort starts to fill the gap between technical research and high-level definition of the future of large-scale multi-agent natural digital twins and Digital Twins.

Acknowledgment

The research presented originated in the support of Tomsk Polytechnic University for conducting studies within the framework of the Creative Initiative No. 46. Negotiations on the distribution, ecology, and technological surplus in the commodity environment of the Russian Federation were held with Watson, C.; Wu, C.; Longo, F.; Thoo, Z.; Bagley, P.; Barros, J.; Mulligan, P.; Chiarini, A.; and Bogoliubov, B. The activity was funded by the Tomsk Polytechnic University development program. A group of scientists and specialists from Russia and the People's Republic of China cooperated in discussing important problems of enhancement of a digital economy based on intelligent technologies in the process of joint participation in the development zero-series project “Digital Earth.” The work was also supported by the Science Foundation for the Development of National Defence Applications of the People's Republic of China under Grant No. 6140D70216. G. S. Yevlampiev participated in the round table “Legal Regulation of Digital Economy as an Important Area of Scientific and Practical Research for the Development Paperless Trade and Economic Relations.”

References

1. Schranz, M., Di Caro, G. A., Schmickl, T., Elmenreich, W., Arvin, F., Şekercioğlu, A., & Sende, M. (2021). Swarm intelligence and cyber-physical systems: Concepts, challenges and future trends. Swarm and Evolutionary Computation, 60, 100762.
2. Strobel, V., Castelló Ferrer, E., & Dorigo, M. (2020). Blockchain technology secures robot swarms: A comparison of consensus protocols and their resilience to Byzantine robots. Frontiers in Robotics and AI, 7, 54.
3. Aditya, U. S. P. S., Singh, R., Singh, P. K., & Kalla, A. (2021). A survey on blockchain in robotics: Issues, opportunities, challenges and future directions. Journal of Network and Computer Applications, 196, 103245.
4. Mashetty, S., Malempati, M., Paleti, S., Adusupalli, B., & Singireddy, J. (2025). A Multidisciplinary Framework for AI and Data-Driven Transformation in Taxation, Insurance, Mortgage Financing, and Financial Advisory: Integrating Cloud Computing, Deep Learning, and Agentic AI for Community-Centric Economic Development. Insurance, Mortgage Financing, and Financial Advisory: Integrating Cloud Computing, Deep Learning, and Agentic AI for Community-Centric Economic Development.
5. Kegeleirs, M., Grisetti, G., & Birattari, M. (2021). Swarm SLAM: Challenges and perspectives. Frontiers in Robotics and AI, 8, 618268.
6. Rakesh, S. K., & Shrivastava, M. (2022). Performance analysis of fault tolerance algorithm for pattern formation of swarm agents. Knowledge-Based Systems, 240, 108020.
7. Wang, K., Liu, Z., Zhu, Z., Qi, G., Yao, J., & Miao, G. (2022). Formation optimization of blockchain-assisted swarm robotics systems against failures based on energy balance. Simulation Modelling Practice and Theory, 120, 102599.
8. Bossens, D. M., Ramchurn, S., & Tarapore, D. (2022). Resilient robot teams: A review integrating decentralised control, change-detection, and learning. Current Robotics Reports, 3, 85–95.

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

9. Tran, V. P., Garratt, M. A., Kasmarik, K., Anavatti, S. G., & Abpeikar, S. (2022). Frontier-led swarming: Robust multi-robot coverage of unknown environments. Swarm and Evolutionary Computation, 75, 101171.
10. Wilson, J., & Hauert, S. (2022). Information transport in communication limited swarms. Artificial Life and Robotics, 27, 632–639.
11. Kummari, D. N., Singireddy, J., Sheelam, G. K., Nandan, B. P., Pandiri, L., Lakkarasu, P., & Dwaraka. (2025, August). Generative AI Models for Process Optimization in Semiconductor Wafer Design and Yield Prediction. In International Conference on Artificial Intelligence: Theory and Applications (pp. 220-233). Cham: Springer Nature Switzerland.
12. Esmalian, A., Wang, W., & Mostafavi, A. (2022). Multi-agent modeling of hazard–household–infrastructure nexus for equitable resilience assessment. Computer-Aided Civil and Infrastructure Engineering, 37, 1491–1520.
13. Buchanan, E., Alden, K., Pomfret, A., Timmis, J., & Tyrrell, A. M. (2023). A study of error diversity in robotic swarms for task partitioning in foraging tasks. Frontiers in Robotics and AI, 9, 904341.
14. Debie, E., Kasmarik, K., & Garratt, M. (2023). Swarm robotics: A survey from a multi-tasking perspective. ACM Computing Surveys, 56(2), 1–38.
15. Peña Queralta, J., Keramat, F., Salimi, S., Fu, L., Yu, X., & Westerlund, T. (2023). Blockchain and emerging distributed ledger technologies for decentralized multi-robot systems. Current Robotics Reports, 4, 43–54.
16. Van Calck, L., Pacheco, A., Strobel, V., Dorigo, M., & Reina, A. (2023). A blockchain-based information market to incentivise cooperation in swarms of self-interested robots. Scientific Reports, 13, 20417.
17. Sun, Y., & Fan, Y. (2023). Improved PBFT algorithm based on K-means clustering for emergency scenario swarm robotic systems. IEEE Access, 11, 121753–121765.
18. Keramat, F., Peña Queralta, J., & Westerlund, T. (2023). Partition-tolerant and Byzantine-tolerant decision-making for distributed robotic systems with IOTA and ROS 2. IEEE Internet of Things Journal.
19. Mashetty, S. (2025). LEVERAGING DEEP LEARNING, NEURAL NETWORKS, AND DATA ENGINEERING FOR INTELLIGENT MORTGAGE LOAN VALIDATION. INTERNATIONAL JOURNAL OF SOCIAL SCIENCE & INTERDISCIPLINARY RESEARCH ISSN: 2277-3630 Impact factor: 8.036, 14(04), 51-65.
20. Cavorsi, M., Sabattini, L., & Gil, S. (2024). Multi-robot adversarial resilience using control barrier functions. IEEE Transactions on Robotics, 40, 797–815.
21. Lee, S. K. (2023). Distributed cohesive configuration controller for a swarm with low-cost platforms. Journal of Field Robotics, 40, 30–56.
22. Salimpour, S., Morón, P. T., Yu, X., Westerlund, T., & Peña Queralta, J. (2023). Exploiting redundancy for UWB anomaly detection in infrastructure-free multi-robot relative localization. Frontiers in Robotics and AI, 10, 1190296.
23. Tian, Y., Chang, Y., Quang, L., Schang, A., Nieto-Granda, C., How, J. P., & Carlone, L. (2023). Resilient and distributed multi-robot visual SLAM: Datasets, experiments, and lessons learned. In 2023 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (pp. 11027–11034). IEEE.
24. Kwa, H. L., Kit, J. L., Horsevad, N., Philippot, J., Savari, M., & Bouffanais, R. (2023). Adaptivity: A path towards general swarm intelligence? Frontiers in Robotics and AI, 10, 1163185.
25. Adusupalli, B., Malempati, M., Paleti, S., Mashetty, S., & Singireddy, J. (2025). Integrated financial ecosystems: AI-driven innovations in taxation, insurance, mortgage analytics, and community investment through cloud, big data, and advanced data engineering. Journal of Information Systems Engineering and Management, 10, 1103-1117.
26. Nasir, M., & Maiti, A. (2024). Adaptive sliding mode resilient control of multi-robot systems with a leader–follower model under Byzantine attacks in the context of the Industrial Internet of Things. Machines, 12(3), 205.
27. Moosavi, S. K. R., Zafar, M. H., & Sanfilippo, F. (2024). Collaborative robots (cobots) for disaster risk resilience: A framework for swarm of snake robots in delivering

P-ISSN: 3050-9556
E-ISSN: 3050-9564
EUROPEAN JOURNAL OF ANALYTICS AND ARTIFICIAL INTELLIGENCE
VOLUME: 04 ISSUE: 01
RECEIVED: JANUARY 03 REVISED: JANUARY 20 ACCEPTED: FEBRUARY 08 PUBLISHED: FEBRUARY 17

first aid in emergency situations. Frontiers in Robotics and AI, 11, 1362294.

28. Yang, S., Zhang, Y., Lu, X., Guo, W., & Miao, H. (2024). Multi-agent deep reinforcement learning based decision support model for resilient community post-hazard recovery. Reliability Engineering & System Safety, 242, 109754.
29. O'Keeffe, J. (2025). Anticipating degradation: A predictive approach to fault tolerance in robot swarms. IEEE Robotics and Automation Letters.
30. Aicha, H., Riadh, H., Guezouli, L., & Moumen, H. (2025). Federated reinforcement learning and deep Q-network: Improving fault tolerance and energy consumption in swarm robotics for mine prospection missions. IEEE Access, 13, 189926–189958.
31. Wang, R., Ma, F., Tang, S., Su, Z., & Xu, C. (2025). Parallel Byzantine fault tolerance consensus for blockchain secured swarm robots. Journal of Field Robotics, 42, 4575–4588.
32. Luo, J., Guo, Y., Cao, T., & Zhu, W. (2025). RobotOBchain: Neighbor observation for Byzantine detection in multi-robot systems. Electronics, 14(24), 4815.
33. Recharla, M. (2024). Antioxidants, Biological Markers, Catalase, Glutathione Peroxidase, Chronic Periodontitis, Saliva, Smokeless tobacco, Smoker. Frontiers in Health Informatics, 13(8), 4999.
34. Ramachandran, R. K., Pierpaoli, P., Egerstedt, M., & Sukhatme, G. S. (2022). Resilient monitoring in heterogeneous multi-robot systems through network reconfiguration. IEEE Transactions on Robotics, 38(1), 126–142.
35. Minelli, M., Panerati, J., Kaufmann, M., Ghedini, C., Beltrame, G., & Sabattini, L. (2020). Self-optimization of resilient topologies for fallible multi-robots. Robotics and Autonomous Systems, 124, 103384.