

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 21

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23



Green Edge Intelligence for Self-Running Infrastructures

^{1st}Phanish Lakkarasu , ^{2nd}Alexander Petrov

Phanish Lakkarasu , Senior Site Reliability Engineer , phanishlakkarasu@gmail.com,
Alexander Petrov , Academic Research Assistant

1. INTRODUCTION

Abstract— Autonomous enterprise operations carry a significant sustainability dimension, one made increasingly urgent as real-world deployments draw near. Existing literature, however, tends to treat their implementation and resulting behaviours qualitatively, rather than as an explicit foundational design concern. In practice, designing, developing, and deploying autonomous systems raises complex sustainability questions — particularly where resource costs are displaced away from the enterprise itself or deferred to later stages such as a system's lifespan and disposal.

While the impact of intelligent technologies on the digital workforce is widely acknowledged, sustainability considerations — especially regarding the labour market — have only recently gained prominence, with Edge Intelligence emerging as a key focal point. These considerations extend beyond resource requirements like energy and materials to encompass support for the circular economy.

In response, frameworks and metrics are emerging to help companies quantify environmental cost-related indicators. Such indicators are essential for mapping the Edge Intelligence of Cyber-Physical Systems (CPS) and their last-mile deployment. Once clearly defined, implemented, and rigorously assessed, these indicators will enable the autonomous enterprise to shape the smart edge of CPS in line with a sustainable transition and digital justice — or, at minimum, to limit the impact on the workforce.

Keywords— Smart cyber-physical infrastructures; autonomous operations; edge intelligence; Edge AI; automation; sustainability; security; privacy; compliance; openness; collaboration.

Governing digital products and services requires a capacity to make and implement decisions based on new information, risks, and regulatory requirements. Stakeholders—vendors, infrastructure decision-makers, application owners, executive management, and legal-compliance teams—want to see that product decisions are risk-aware, acted on in a timely manner, and supported by guidance demonstrating accountability. Operationalizing these demands involves establishing playbooks that govern the adoption of ever-pervasive cloud-based technologies and follow a digital-governance approach, with a focus on making the decision process transparent and auditable.

Decision intelligence combines classic decision-making activities featuring risk and reward while coordinating the relevant actors, supporting technologies, and information. Governance concerns determine who has the right to make or influence specific decisions, security and legal teams need to address the manner of collecting and processing data, and the responsible-innovation paradigm ensures that the technology adoption decision process is transparent and ethically responsible. Playbooks articulate the entire process of digital product adoption in a rational manner, emphasizing the principles of alignment, verification, and specification around the product audit track that must be followed.

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 21

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23

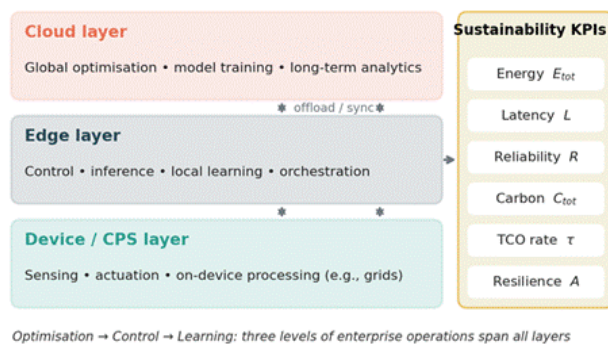


Fig. 1. Layered edge-intelligence architecture for autonomous enterprise operations, linked to the six sustainability KPIs.

2. Theoretical Foundations of Decision Intelligence in Digital Infrastructure

Decision intelligence integrates theory and practice across disciplines to inform decisions about complex systems, such as Digital Infrastructure. Combining decision theory, the governance of data, and Risk Governance and Compliance (GRC) in Information Technology, creates an agenda for research and practice through the lens of governed digital infrastructure. By distilling utility, uncertainty, and trade-offs, decision theory reveals the factors determining the desirability of digital infrastructure products and services. Theories of governance, risk, and compliance highlight the processes and criteria that, if followed, contribute to the socially, politically, and economically acceptable adoption of these products and services.

Decision Theory provides insight into how products and services in a digital infrastructure context should be assessed and compared. Digital Infrastructure is complex; products and services are made up of many components, dependent and independent alike. A Risk-Aware approach is needed as Infrastructure decisions are technical, operational, and technology decisions driven by data or by data products used by external-facing user communities; public trust is essential for Equity and Safety in Technology Adoption. Decisions are often multidimensional; multiple stakeholder groups will be involved in governance. Outputs require both formal approval and public acceptance. At all times, a transparent, published approval decision trail with associated risk analysis

supports ongoing post-implementation audit, serves as a basis for ongoing stakeholder trust, and provides an alignment mechanism for Infrastructure Roadmaps and Project Prioritization.

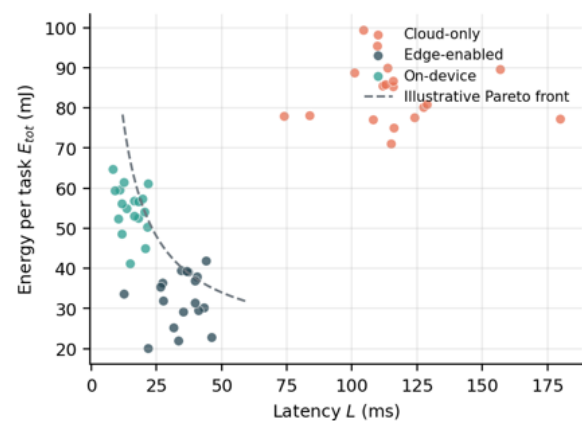


Fig. 2. Latency–energy trade-off by deployment site (illustrative data).

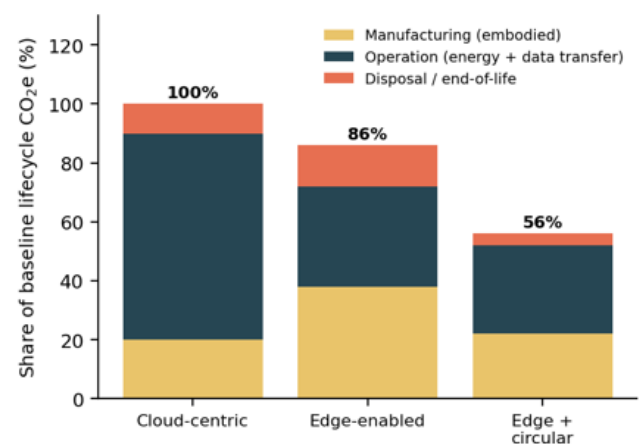


Fig. 3. Lifecycle carbon by stage, indexed to a cloud-centric baseline (illustrative data).

3. Governance and Compliance in Technology Adoption

Governance structures, policy instruments, and regulatory regimes form the governance ecosystem affecting the

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 21

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23



adoption of technology products. While traditional decision-making focuses on technical problems, both public and private sector governance create compliance requirements for technology adoption, imposing a heavy burden on decision makers. In the public sector, these requirements—identified through process mapping—include approval and oversight requirements for policy, procurement, and expenditure; legislative compliance for procurements and expenditure; fiscal responsibility oversight; data protection; privacy and surveillance; data security; information security; disability; official transport; and ethical finance. In total, they comprise 23 decision points that add significant time overhead to technology adoption. Aligning with the intent of these requirements through collaborative risk assessment at the product or service level, rather than the jurisdictional level, would facilitate timely deployments and likely satisfy compliance.

Governance comprises rules and regulations within both public and private sectors that specify what must be done, how it should be done, and by whom. Decision makers face complex questions when procuring and adopting technology that allows faster, cheaper, and better delivery of services and that addresses stakeholder concerns. Yet products creating significant data privacy and security risks with respect to the offering business or agent are often adopted unaudited or uncleared, with risk assessments avoided or superseded by processes. Even the private sector, which has generally adopted a business-first ethos, should engage risk assessment as a core component of Governance Risk and Compliance procedures.

Mathematical Formulas:

Equations (1)–(6) formalise the KPI definitions in Section 4 of the paper. Equations (7)–(10) support the composite-metric, trade-off and risk-decision discussion.

$$E_{\text{tot}} = \sum_{i \in \text{edge}} E_i + \sum_{j \in \text{cloud}} E_j \quad (1)$$

Total energy: all edge and cloud resources used to process one enterprise task.

$$L = t_{\text{reply}} - t_{\text{request}} = L_{\text{tx}} + L_{\text{queue}} + L_{\text{proc}} \quad (2)$$

Latency: client request to first reply across the edge–cloud path (transmission, queuing, processing).

$$R = \frac{N_{\text{success}}}{N_{\text{requests}}} \quad (3)$$

Reliability: long-term share of requests executed successfully.

$$C_{\text{tot}} = \sum_k E_k \cdot CI_k + C_{\text{emb}} + C_{\text{eol}} - C_{\text{offset}} \quad (4)$$

Net carbon footprint: operational energy $\times$ grid carbon intensity (CI), plus embodied and end-of-life emissions, minus offsets/reuse credits.

$$\tau = \frac{C_{\text{deploy}} + C_{\text{operate}} + C_{\text{scale}}}{T_{\text{op}}} \quad (5)$$

Total cost of ownership over deployment, operation and scaling, normalised by operation time.

$$A = \frac{T - T_{\text{down}}}{T} \times 100 \% \quad (6)$$

Resilience: percentage of time the business service is up (no down-period).

$$S = \sum_m w_m \tilde{x}_m, \text{ with } \sum_m w_m = 1 \quad (7)$$

Composite sustainability index; $\tilde{x}_m$ is metric m min–max normalised to $[0,1]$ (inverted for cost-type metrics such as E , L , C , τ).

$$\min (E_{\text{tot}}, L, C_{\text{tot}}, \tau) \text{ s.t. } R \geq R_{\text{min}}, A \geq A_{\text{min}} \quad (8)$$

Deployment trade-off: choose the edge/cloud placement that minimises cost-type KPIs while meeting reliability and resilience floors.

$$EU(a) = \sum_s p(s) \cdot u(a, s) \quad (9)$$

Decision theory (Sections 2–4): expected utility of option a under uncertain scenarios s .

$$\rho_{\text{res}} = P_r \cdot I_r \cdot (1 - \eta) \quad (10)$$

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 21

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23



Residual risk after controls: $\text{likelihood} \times \text{impact}$,
reduced by control effectiveness $\eta \in [0,1]$.

4. Risk Assessment Frameworks for Product Decisions

Risk assessment frameworks tailored to product decisions encompass technology threat modeling, product impact analysis, and evaluation of the residual risks associated with technology adoption. The practical details of each framework are addressed in turn.

The risk taxonomy identifies the key categories, the qualitative scoring rubrics specify the question sets that guide risk scoring, and the quality-assessment guidelines articulate the recommended standards for inputs into risk evaluations. Further, enablers and challenges for uncertainty quantification and sensitivity analysis are described. Decision envelopes, guardrails, and fallback options for product choices are proposed, and considerations for scenario planning and stress-testing methodologies are outlined. Together, these materials provide a structured means of assessing risk in the adoption of third-party products and services.

A product's cyber threat landscape encompasses vulnerabilities that could be exploited, pathways through which attackers might exploit them, and business partners or other third parties that might affect the likeRecent advances in the adoption of edge infrastructures create an opportunity for incorporating near-detection intelligence in digital operations and services in the broad context of smart cyber-physical infrastructures. Edge Intelligence enables the realization of autonomous enterprise operations in a wide range of application domains. In the context of these infrastructures—comprised of device and platform ecosystems that support the cooperation of people, machines, and software agents within their environment—it's expected that planning and decision-making can be carried out by distributed intelligent agents controlled in a decentralized fashion. However, the reliance on the automatic interaction of systems, for example in decision-making processes, poses significant sustainability concerns. The efficiency of data pipelines, the longevity of physical components, the synergy of the system's autonomous units, and, consequently, the total cost of ownership of autonomous operations should be

addressed, together with the environmental aspects of such implementations.

Together with decentralized operational models, integrating the sustainability of the produced solutions into feasible life-cycle evaluation and the design of evaluation protocols, benchmarks, and experimentation setups enable an objective study of the ecological aspects of deploying Edge Intelligence to enable autonomous operations within smart cyber-physical infrastructures. The consideration of quantitative metrics that target energy efficiency, latency trade-offs, reliability, lifespan of the providing components, and total cost of ownership offer a comprehensive view of the ecological impact. An integrated dashboard supports the analysis of data collected to validate environmental claims. The exploration of the adequacy of the produced composite metrics for monitoring enables infeasibility analysis. Capturing the trade-offs and conjunctions between performance, cost, and ecological impact suggests directions for future investments and accelerates the long-term viability of these systems.

TABLE 1. Sustainability KPIs for edge intelligence in smart CPS (Section 4)

Dimension	KPI	Symbol	Definition (as in paper)	Unit
Environmental	Total energy use	E_{tot}	Energy consumed by all edge and cloud resources for the selected task	J / kWh per task
Environmental	Latency	L	Time between client request and first reply in the edge-cloud environment	ms
Environmental	Reliability	R	Long-term successful task executions relative to requests	% (0–1)

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 21

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23



Environmental	Carbon footprint	C_{tot}	Net carbon emissions of an edge-automated smart enterprise operation	kg CO ₂ e
Economic	Total cost of ownership	τ	Deployment + operation + scaling costs, normalised by operation time	currency / h
Economic	Resilience	A	Long-term service maintenance: share of time without a down-period	% uptime

TABLE 2. Enterprise operation levels and typical edge-cloud placement (Sections 2–3)

Level	Typical functions	Preferred site	Main KPI driver
Optimisation	Resource allocation, energy-hungry task scheduling, risk/cost/compliance evaluation	Cloud / edge	E_{tot} , τ
Control	Sensing-actuation loops (open/closed), supervisory control, first-order control inputs	Edge / on-device	L, R
Learning	Anomaly detection, state forecasting, prognosis, lifecycle assessment, failure RUL, impact	Edge (inference), cloud (training)	C_{tot} , E_{tot}

5. Security, Privacy, and Compliance in Edge Environments

A novel threat model for edge-enabled cyber-physical systems incorporates aspects specific to dependence on edge computing resources and distributed deployment, and proposes security controls to mitigate identified risks. Security controls span data governance, edge node hardening, and secure orchestration. Furthermore, zero-trust principles and incident response capabilities are advocated. The planned deployment of smart distribution grids serves as an example threat model within which relevant controls are aligned to meet specific privacy-preservation concerns and compliance requirements.

Smart distribution grids are posited as one representative use case for autonomous operations across edge-CPS environments. Such environments necessitate consideration of risk factors, security controls, and governance measures in the design and development of enterprise processes. Given the use of enterprise and personal data, prioritizing data governance with due respect for privacy-preservation is essential. The cross-cutting nature of edge computing also demands particular attention to compliance and regulatory requirements. Addressing the associated threat models, security-defence mechanisms, and mitigation techniques thus ensures that users, operators, and involved stakeholders are aware of possible risks when operating within such environments.

TABLE 3. Edge-CPS security and privacy controls (Section 5)

Control area	Purpose	Protects
Data governance	Rules for collecting, processing and sharing enterprise and personal data	Privacy, compliance
Edge node hardening	Reduce attack surface of exposed, resource-constrained nodes	Integrity, availability
Secure orchestration	Trusted task distribution among	Integrity, confidentiality

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 21

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23



	distributed devices and agents	
Zero-trust principles	Continuous verification of every user, device and service	Confidentiality, integrity
Incident response	Detect, contain and recover from attacks; support audit	Availability, accountability

6. Conclusion

Security and privacy dimensioning in advanced edge environments constitutes an essential component of responsible AI in distributed infrastructures characterized by autonomous decision-making. However, ensuring the confidentiality, integrity, and availability of the datasets leveraged and the decision-making processes performed at the edge represents a significant challenge due to the open and decentralized nature of these environments. Indeed, advanced edge systems are more susceptible to different security threats and vulnerabilities than traditional centralized cloud systems.

Building on this motivation, this research section identifies and investigates the unique security, privacy, and compliance aspects of edge-enabled autonomous operations. More specifically, it identifies the distinct security threats, risk factors, and privacy considerations associated with the edge, and discusses how these aspects can be effectively managed to foster trust in deployed solutions and, consequently, their adoption.

The resulting body of knowledge encompasses a broad set of security dimensioning strategies across different layers and phases of the distributed infrastructure. Combining principles and techniques from different areas of distributed systems such as edge computing, network security, and privacy preservation, the proposed security-enhanced risk management framework forms a comprehensive and effective reference for responsible-edge enabled autonomous operations. Finally, its applicability is illustrated through a practical case study addressing a multi-tenant edge support architecture for distributed AI-based traffic management.

REFERENCES

1. Zhou, C., Sun, Y., Liu, H., & Zhang, Z. (2020). Edge intelligence: The confluence of edge computing and artificial intelligence. *IEEE Internet of Things Journal*, 7(8), 7457–7469.
2. Xu, D., Li, T., Li, Y., Su, X., Tarkoma, S., Jiang, T., Crowcroft, J., & Hui, P. (2020). Edge intelligence: Architectures, challenges, and applications. *arXiv*.
3. Li, W., Wang, X., Zhang, Y., & Wang, L. (2020). Edge intelligence: Challenges and opportunities. In 2020 International Conference on Computer, Information and Telecommunication Systems (CITS).
4. Khan, L. U., Yaqoob, I., Tran, N. H., Kazmi, S. M. A., Dang, T. N., & Hong, C. S. (2020). Edge-computing-enabled smart cities: A comprehensive survey. *IEEE Internet of Things Journal*, 7(10), 10235–10254.
5. Malhotra, A., Niharika, D. S., Mangalampalli, B. M., Nema, S., Gupta, Z., & Kriplani, K. (2026, June). Distributed and Edge AI for Continuous and Context-Aware Healthcare Intelligence. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-6). IEEE.
6. Jang, Y., Na, J., Jeong, S., & Kang, J. (2020). Energy-efficient task offloading for vehicular edge computing: Joint optimization of offloading and bit allocation. In 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring).
7. Zhang, X., & Debroy, S. (2020). Energy efficient task offloading for compute-intensive mobile edge applications. In 2020 IEEE International Conference on Communications (ICC).
8. Zhang, Y., Wang, Y., Chen, X., & Li, Z. (2021). Energy-efficient task offloading and resource allocation via deep reinforcement learning for augmented reality in mobile edge networks. *IEEE Internet of Things Journal*, 8(13), 10843–10856.
9. Seenu, A., Kolla, S. H., Aitha, A. R., Amistapuram, K., Abhireddy, N., & Yandamuri, U. S. (2026, June). Agentic Enterprise Intelligence: A Unified Architecture for Secure RAG-Enabled LLM Automation in Insurance Risk and Fraud Ecosystems. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-5). IEEE.
10. Chen, X., Jiao, L., Li, W., & Fu, X. (2021). Efficient multi-user computation offloading for mobile-edge cloud computing. *IEEE/ACM Transactions on Networking*, 29(2), 779–792.
11. Brogi, A., Carrasco, J., Durán, F., Pimentel, E., & Soldani, J. (2022). Self-healing trans-cloud applications. *Computing*, 104, 809–833.
12. Wang, X., Han, Y., Leung, V. C. M., Niyato, D., Yan, X., & Chen, X. (2020). Convergence of edge computing and deep learning: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 22(2), 869–904.

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING

VOLUME: 04 ISSUE: 03

RECEIVED: JULY 07

REVISED: JULY 21

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23



13. Penaka, B. (2026). AUTONOMOUS MULTI-AGENT AI FRAMEWORK FOR END-TO-END CLINICAL DECISION SUPPORT AND CARE COORDINATION. *Genetics and Molecular Research*.
14. Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Niyato, D. (2022). 6G Internet of Things: A comprehensive survey. *IEEE Internet of Things Journal*, 9(1), 359–383.
15. McEnroe, P., Wang, S., & Liyanage, M. (2022). A survey on the convergence of edge computing and AI for UAVs: Opportunities and challenges. *IEEE Internet of Things Journal*, 9(17), 15435–15459.
16. Mahadevan, S. (2026). Governed Serverless Automation Ecosystem for AI-Driven Enterprise Integration and Sustainable Cloud Operations. *International Journal of Computer Information Systems and Industrial Management Applications*, 18(16s), 1561-1570.
17. Mahenge, M. P. J., Li, C., & Sanga, C. A. (2022). Energy-efficient task offloading strategy in mobile edge computing for resource-intensive mobile applications. *Digital Communications and Networks*, 8(6), 1048–1058.
18. Tajallifar, M., Ebrahimi, S., Javan, M. R., Mokari, N., & Chiaraviglio, L. (2022). Energy-efficient task offloading under E2E latency constraints. *IEEE Transactions on Communications*, 70(3), 1711–1725.
19. Venkateswara Rao Movva. (2026). Self-Healing Retail Platforms Using Agentic AI: Autonomous Detection, Reasoning, and Remediation of Cloud Infrastructure Failures. *International Journal of Special Education*, 41(20s), 1198–1204. Retrieved from <https://internationalsped.com/index.php/ijse/article/view/6139>
20. Azizi, S., Othman, M., & Khamfroush, H. (2023). DECO: A deadline-aware and energy-efficient algorithm for task offloading in mobile edge computing. *IEEE Systems Journal*, 17(1), 952–963.
21. Bullo, M., Jardak, S., Carnelli, P., & Gündüz, D. (2023). Sustainable edge intelligence through energy-aware early exiting. *arXiv*.
22. Singh, K. U., Gupta, S. K., Dubey, Y., & Mangalampalli, B. M. (2026, June). Enhancing Healthcare Cyber Defense with Machine Learning-Based Attack Prediction and Prevention. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-6). IEEE.
23. Arroba, P., Buyya, R., Cárdenas, R., Risco-Martín, J. L., & Moya, J. M. (2024). Sustainable edge computing: Challenges and future directions. *Software: Practice and Experience*, 54(11), 2272–2296.
24. Ben Cheikh, S., & Sigg, S. (2024). Towards green edge intelligence. In *IoT 2023: Proceedings of the 13th International Conference on the Internet of Things* (pp. 197–199). ACM.
25. Li, J., Wei, H., Liu, J., & Liu, W. (2024). FSLEdge: An energy-aware edge intelligence framework based on federated split learning for industrial Internet of Things. *Expert Systems with Applications*, 255, 124564.
26. Li, Y., Qin, D., Poor, H. V., & Wang, Y. (2024). Introducing edge intelligence to smart meters via federated split learning. *Nature Communications*, 15, 9044.
27. Potturi, P. (2026). Agentic Business Intelligence Architecture for Autonomous Data Exploration, Insight Generation, and Strategic Decision Orchestration. *International Journal of Computer Information Systems and Industrial Management Applications*, 18(22s), 536-542.
28. Chen, K., Sun, Y., Zheng, S., Yang, H., & Yu, P. (2024). Online collaborative energy-network resource scheduling for WPT-enabled green edge computing. *IEEE Transactions on Green Communications and Networking*, 8(2), 601–618.
29. Bibri, S. E., Huang, J., Jagatheesaperumal, S. K., & Krogstie, J. (2024). The synergistic interplay of artificial intelligence and digital twin in environmentally planning sustainable smart cities: A comprehensive systematic review. *Environmental Science and Ecotechnology*, 20, 100433.
30. Wang, H., & Wang, Y. (2024). Smart cities net zero planning considering renewable energy landscape design in digital twin. *Sustainable Energy Technologies and Assessments*, 63, 103629.
31. Liu, K., & Zhang, S. (2024). Smart cities stochastic secured energy management framework in digital twin: Policy frameworks for promoting sustainable urban development in smart cities. *Sustainable Energy Technologies and Assessments*, 65, 103720.
32. Suprith, M., Davuluri, P. N., Paramasamy, S., Yandamuri, U. S., & Motamary, S. (2026, June). AI-Enabled Business Process Reengineering for Agile and Data-Driven Organizations. In 2026 5th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-6). IEEE.
33. Chen, L., Li, X., & Zhu, J. (2024). Carbon peak control for achieving net-zero renewable-based smart cities: Digital twin modeling and simulation. *Sustainable Energy Technologies and Assessments*, 65, 103792.
34. Zhang, H., & Feng, X. (2024). Reliability improvement and landscape planning for renewable energy integration in smart cities: A case study by digital twin. *Sustainable Energy Technologies and Assessments*, 64, 103714.
35. Guo, Y., Fu, Y., Zhang, Y., & Quek, T. Q. S. (2024). Age-of-information and energy optimization in digital twin edge networks. In 2024 IEEE Global Communications Conference (GLOBECOM) (pp. 3194–3200).
36. Xu, H., Omitaomu, F., Sabri, S., Zlatanova, S., Li, X., & Song, Y. (2024). Leveraging generative AI for urban digital twins: A scoping review on the autonomous generation of urban data,

AMERICAN ONLINE JOURNAL OF SCIENCE AND ENGINEERING

VOLUME: 04 ISSUE: 03



RECEIVED: JULY 07

REVISED: JULY 21

ACCEPTED: AUGUST 04

PUBLISHED: AUGUST 23

scenarios, designs, and 3D city models for smart city advancement. *Urban Informatics*.

37. Pazienza, A., Baselli, G., Vinci, D. C., & Trussoni, M. V. (2024). A holistic approach to environmentally sustainable computing. *Innovations in Systems and Software Engineering*, 20, 347–371.
38. Konda, S. K. (2024). Carbon-native DCIM architectures for AI data centers: Autonomous infrastructure control via smart grid intelligence. *World Journal of Advanced Research and Reviews*, 21(1), 3008–3318.
39. Zhou, Y., & Chen, X. (2025). Edge intelligence: Edge computing for 5G and the Internet of Things. *Future Internet*, 17(3), 101.
40. Ellenki, R. R., & Venkatesh, P. (2026). Collaborative AI Agent Architecture for Autonomous Retail Inventory and Allocation Management. *International Journal of Computer Information Systems and Industrial Management Applications*, 18(23s), 933-940.
41. Bo, Y., Feng, J., Zhang, S., & Leng, B. (2025). Multi-agent reinforcement learning with graph representation for green edge-cloud computation offloading. *Computer Communications*, 243, 108176.
42. Zhou, X., Guan, X., Sun, D., Zhang, X., Zhang, Z., & Ohtsuki, T. (2025). Heterogeneous multi-agent deep reinforcement learning based low carbon emission task offloading in mobile edge computing. *Computer Communications*, 234, 108089.
43. Liu, H., Huang, L., Tian, Y., Ding, J., Yin, X., & Zhang, G. (2025). Tensor-based task allocation using multi-objective optimization in GECC environment. *Computer Communications*, 243, 108316.
44. Li, J., Liu, Y., Wang, X., & Chen, Z. (2025). Energy-efficient dynamic offloading and resource management for intelligent edge computing systems. *IEEE Access*, 13, 127489–127506.