Original research article / Originalus mokslinis straipsnis
Vol. 1 No. 10 (2025): Gruodis

Application of Information Technologies in the Control of Technical Systems

[1] Cebrayil Huseynov

Accepted: 12.05.2025
Published: 12.09.2025
https://doi.org/10.69760/portuni.0110013

Abstract; The integration of modern information technologies into technical control systems is fundamentally transforming industrial automation and infrastructure management. This article provides a theoretical and global examination of how IoT connectivity, cloud–edge computing, artificial intelligence, and digital twin technologies are reshaping control architectures and operational practices. Traditional isolated SCADA environments are evolving into interconnected, data-centric ecosystems capable of real-time monitoring, predictive analytics, and adaptive decision-making. The analysis highlights the substantial benefits of this transition—enhanced automation responsiveness, improved situational awareness, reduced downtime, and significant gains in energy and resource efficiency. At the same time, the study identifies critical challenges, including cybersecurity vulnerabilities, interoperability complexities, and growing system heterogeneity requiring advanced skills and robust governance. Emerging trends such as AI-driven autonomy, 5G/6G-enabled connectivity, digital twin ecosystems, and Industry 5.0 human-centric principles suggest a future of increasingly intelligent, sustainable, and resilient control systems. The findings underscore that successful adoption depends on coordinated technological innovation, strong cybersecurity practices, and cross-disciplinary workforce development.

Keywords: *Intelligent control systems, Industrial IoT, Digital twins, Cyber-physical automation*

Introduction

The integration of modern information technologies into technical control systems is reshaping industrial automation and smart infrastructure worldwide. With the rise of Industry 4.0, formerly isolated operational technology (OT) systems are increasingly merging with information technology (IT), enabling real-time data exchange, remote supervision, and global automation (Frank et al., 2019; Lu, 2017). Cyber-physical systems, IoT connectivity, and advanced networking now allow factories, utilities, and transportation systems to operate as interconnected, data-driven ecosystems rather than siloed units (Lee et al., 2015). This shift transforms monitoring and control from manual, local operations to integrated digital environments supported by analytics and automation (Farooq et al., 2023; Venanzi et al., 2025).

[1] Huseynov, C. Master's Student, Nakhchivan State University, Azerbaijan. Specialty: Application of Information Technologies in the Management of Technical Objects. Email: cbrayilhuseynov83@gmail.com. ORCID: https://orcid.org/0009-0009-8630-960X

This article provides a concise theoretical overview of major IT innovations applied to technical control systems, highlighting global developments in IoT, SCADA modernization, cloud-edge architectures, AI-enhanced automation, and digital twins. Benefits such as improved efficiency, real-time visibility, and predictive capability are discussed alongside challenges including cybersecurity, interoperability, and system complexity (Wali & Alshehry, 2024; Enemosah & Ifeanyi, 2024). The review positions these technologies within the broader evolution from closed control networks toward open, intelligent industrial ecosystems.

Theoretical Background: From Traditional Control to Industry 4.0

Technical control systems—traditionally implemented using SCADA, DCS, and PLC-based architectures—were historically isolated, proprietary, and optimized for reliability rather than connectivity (Rustamova & Rustamov, 2024). Classical SCADA models involved field sensors and actuators communicating only with onsite supervisory servers, limiting interoperability and external data exchange (Enemosah & Ifeanyi, 2024).

Industry 4.0 has accelerated IT/OT convergence, enabling industrial equipment to communicate through IIoT devices, cloud services, and cyber-physical systems (Kagermann et al., 2013; Farooq et al., 2023). IoT integration allows remote monitoring, fine-grained telemetry, and cross-site visibility (Chang et al., 2021). CPS technology further links digital computation with physical processes, allowing software to directly sense and control machinery in real time (Lee et al., 2015).

Modern architectures increasingly adopt open communication standards such as OPC UA to overcome vendor lock-in and facilitate interoperability across industrial networks (Venanzi et al., 2025). As systems become interconnected, they support enterprise-level analytics, machine learning–based optimization, and predictive maintenance—but also inherit greater cybersecurity exposure (Wali & Alshehry, 2024; Moxa, 2021).

Overall, the transition from isolated SCADA systems to integrated Industry 4.0 platforms establishes the technological foundation for advanced control, automation, and global system intelligence that define modern technical environments.

Cloud Computing and Industrial Automation

Cloud computing has become a central pillar of digital transformation in industrial automation, offering scalable storage, high-capacity processing, and remote accessibility for technical control systems. As IIoT deployments generate massive data streams, cloud platforms provide elastic resources that support sensor data archiving, supervisory analytics, and AI-driven optimization without the need for extensive on-premise infrastructure (Chang et al., 2021; Simio, 2025). Centralizing data in cloud environments also enables organizations to monitor distributed operations from a unified interface, compare performance across sites, and coordinate predictive maintenance strategies globally (InHand Networks, 2025; Venanzi et al., 2025).

Cloud adoption introduces modern software paradigms—service-oriented architectures, APIs, virtualization, and containerization—into traditionally static OT domains (Ness, 2025; Rustamova & Rustamov, 2024). These trends support emerging models such as SCADA-as-a-Service and virtualized control components. However, they also raise challenges. Industrial operators must manage latency

constraints, ensure continuous local control through hybrid cloud-edge architectures, and address cybersecurity risks inherent in multi-tenant cloud environments (Wali & Alshehry, 2024; Moxa, 2021). Private clouds, VPNs, and encryption are often used to secure critical data.

Despite concerns, cloud computing significantly enhances operational intelligence. Cloud-based analytics reduce downtime, improve production efficiency, and enable enterprise-wide optimization—demonstrating why cloud integration is increasingly essential in modern control ecosystems (Frank et al., 2019; Farooq et al., 2023).

Edge and Fog Computing for Real-Time Control

While cloud systems provide global visibility, edge computing addresses the need for low-latency, real-time control by processing data near its source. In industrial environments, edge devices (smart PLCs, gateways, or embedded controllers) execute control logic locally, ensuring millisecond-level responses and safe operation even when remote connectivity is limited (Ness, 2025; Enemosah & Ifeanyi, 2024). Fog computing extends this concept by creating intermediate processing layers between the edge and cloud, distributing computation across the network continuum.

Edge intelligence is particularly valuable for safety-critical applications such as anomaly detection or equipment protection. Models trained in the cloud can be deployed on edge hardware to autonomously identify faults and initiate immediate corrective actions, reducing reliance on high-bandwidth or high-latency cloud communication (Rustamova & Rustamov, 2024; Chang et al., 2021). This approach also minimizes network load by transmitting only aggregated or event-based data upstream.

Edge and fog architectures improve cybersecurity by keeping sensitive operational data on-site and ensuring continued local control if cloud links fail (Wali & Alshehry, 2024). They also lower operating costs by filtering data before transmission and reducing downtime through faster local decision-making. Industry analyses consistently emphasize that modern control systems succeed by combining cloud-level analytics with edge-level autonomy, rather than favoring one architecture exclusively (Farooq et al., 2023; Venanzi et al., 2025).

In summary, edge and fog computing extend the capabilities of cloud systems, enabling responsive, resilient, and scalable industrial control. Together, they form the backbone of next-generation intelligent automation.

Artificial Intelligence and Machine Learning in Control Systems

Artificial intelligence (AI) and machine learning (ML) are reshaping industrial control by enabling systems to learn, optimize, and adapt rather than simply execute fixed logic. Their adoption—often described as Industrial AI—supports predictive analytics, anomaly detection, real-time optimization, and intelligent decision support across manufacturing, utilities, and critical infrastructure (Rustamova & Rustamov, 2024; Farooq et al., 2023).

A major industrial application is **predictive maintenance**. ML models trained on historical vibration, temperature, or power signatures can detect early indicators of equipment degradation. When incorporated into SCADA or IIoT architectures, these models generate proactive alerts and reduce unplanned downtime (Simio, 2025; Frank et al., 2019). AI-enabled anomaly detection similarly

improves product quality and operational reliability by identifying abnormal behavior faster and more accurately than human operators.

AI is also emerging in **real-time control**. Reinforcement learning and neural network–based controllers can optimize energy usage, tune nonlinear processes, and respond dynamically to changing conditions. These methods outperform fixed control logic in complex environments and can coordinate multiple control loops simultaneously (Chang et al., 2021; Enemosah & Ifeanyi, 2024).

Another impactful area is **decision support**. Modern SCADA/HMI systems increasingly integrate AI analytics to forecast trends, highlight risks, and recommend corrective actions. For example, AI can predict overload conditions in power grids or forecast quality deviations on production lines, helping operators act before issues escalate (Rustamova & Rustamov, 2024).

However, the use of AI introduces challenges: industrial datasets are often noisy and incomplete, and deploying sophisticated models on edge devices requires compute-efficient algorithms (Moxa, 2021). Ensuring trustworthy, interpretable AI output is essential, especially in safety-critical domains.

Despite these hurdles, evidence consistently shows that AI improves efficiency, reduces downtime, and enhances operational sustainability across technical systems worldwide (Farooq et al., 2023; Simio, 2025).

Digital Twins and Simulation in Control

Digital twins—virtual replicas of physical assets or processes—have become foundational tools in advanced control architectures. By synchronizing real-time IoT data with simulation models, digital twins enable continuous monitoring, predictive analytics, and scenario-based optimization (Mendonça et al., 2022; Simio, 2025).

A digital twin provides a safe environment for **what-if simulations**, allowing engineers to test process changes, validate control logic, or optimize production parameters without disrupting physical operations. This accelerates commissioning, reduces risk, and supports data-driven decision-making across the system lifecycle (Lee et al., 2015; Lu, 2017). Many companies report significant reductions in operational costs and time-to-market when digital twins are integrated into their automation ecosystems.

Digital twins also enhance **predictive maintenance and anomaly detection** by comparing real system behavior with simulated expectations. Deviations—such as rising energy consumption or abnormal thermal patterns—signal emerging faults earlier than traditional monitoring methods (Mendonça et al., 2022).

More advanced implementations integrate AI, forming **intelligent digital twins** capable of adaptive optimization. For example, HVAC or process-control twins can automatically adjust parameters to improve efficiency, effectively closing the loop between simulation and real-world control.

Challenges remain, including model accuracy over time, high data integration demands, and cybersecurity concerns. Nevertheless, rapid technological progress—particularly in cloud computing, IIoT, and edge analytics—is driving widespread adoption. Analysts forecast that digital twins will become standard across manufacturing, energy, transportation, and infrastructure systems within this decade (InHand Networks, 2025; Venanzi et al., 2025).

In essence, digital twins extend the reach of information technologies into every stage of technical system management, enabling deeper insight, safer experimentation, and more intelligent control decisions.

Benefits for Automation, Monitoring, and Efficiency

The combined use of IoT, edge computing, cloud platforms, AI, and digital twins is significantly enhancing automation, monitoring, and operational efficiency in modern technical systems. Each technology contributes unique capabilities; together they create highly responsive, data-driven, and adaptive control environments (Chang et al., 2021; Frank et al., 2019).

Enhanced Automation and Responsiveness.

IoT sensors generate continuous, high-resolution data streams, while edge processors analyze this data immediately to support real-time control decisions. This reduces latency and eliminates dependence on centralized systems, allowing equipment to react almost instantaneously to disturbances (Ness, 2025; Moxa, 2021). AI-based controllers further improve responsiveness by learning optimal behaviors over time and adapting to changing conditions. Predictive analytics help increase throughput and reduce waste by anticipating deviations before they affect production (Simio, 2025).

Improved Monitoring and Situational Awareness.

Cloud-based integration and IoT connectivity offer operators a unified, real-time view of system performance across sites. Dashboards enriched with AI highlight anomalies, trends, or risks, improving situational awareness and speeding up decision-making (Rustamova & Rustamov, 2024). Digital twins enhance monitoring by comparing live system data with simulated expectations, enabling forward-looking assessments and earlier interventions (Mendonça et al., 2022). These capabilities have been shown to reduce defect rates and improve quality in smart manufacturing.

Efficiency and Optimization Gains.

AI-driven optimization improves energy consumption, resource efficiency, and asset utilization. Predictive maintenance ensures timely interventions, extending equipment life and reducing downtime (Farooq et al., 2023). Digital twins support scenario testing, scheduling optimization, and process tuning, often resulting in double-digit improvements in throughput or energy performance (InHand Networks, 2025). Interoperability standards such as OPC UA and MQTT further boost efficiency by reducing integration work and enabling seamless data exchange.

Overall, the integration of these technologies shifts automation from rigid programming to adaptive, self-optimizing systems. Human operators increasingly supervise and refine intelligent processes rather than manually adjusting controls, resulting in consistently improved productivity and reliability (Frank et al., 2019; Simio, 2025).

Challenges in Implementing Intelligent Control Systems

Despite substantial benefits, organizations face significant challenges when applying advanced IT in control environments—including cybersecurity risks, interoperability barriers, and increased system complexity.

Cybersecurity Vulnerabilities.

Connecting SCADA, IoT devices, and cloud systems expands the attack surface. Legacy controllers often lack encryption or authentication, and misconfigured cloud interfaces create additional risks (Wali & Alshehry, 2024). Cyber incidents have shown that attacks can propagate from IT networks into OT systems, threatening both data and physical processes. Effective security requires layered defenses, including segmentation, strong access control, encryption, and continuous monitoring following ICS security standards (Venanzi et al., 2025; Rustamova & Rustamov, 2024).

Interoperability and Integration Challenges.

Industrial environments commonly contain heterogeneous equipment from many vendors. Integrating legacy systems with modern IoT and cloud platforms often requires custom gateways, protocol translation, and reconciliation of inconsistent data models (Farooq et al., 2023). Surveys show that interoperability issues remain a primary barrier to IIoT adoption, with significant value lost when systems cannot communicate reliably (InHand Networks, 2025). While standards like OPC UA and MQTT help, not all vendors comply or update older equipment.

System Complexity and Maintainability.

Integrating IoT, AI, cloud services, and edge computing produces highly complex architectures. Troubleshooting becomes more difficult because failures may originate from sensors, networks, AI models, or edge devices. AI outputs also raise concerns in safety-critical environments due to limited interpretability (Chang et al., 2021). Maintaining these systems requires workers skilled in both IT and OT disciplines—a gap many organizations struggle to address (Frank et al., 2019).

Additional Concerns.

Data privacy, regulatory constraints, and the challenge of managing thousands of IoT devices add further burden. Critical industries must validate autonomous functions rigorously, and many maintain manual backups to preserve safety. Scaling intelligent control systems from pilot projects to enterprise-wide deployments also requires careful planning and governance (Venanzi et al., 2025).

In summary, the transition to intelligent control systems introduces substantial cybersecurity, integration, and organizational challenges. Addressing them requires coordinated IT/OT strategies, standardized interfaces, upskilling of personnel, and robust security frameworks. Organizations that navigate these challenges effectively gain significant competitive advantage, while failure to manage them can undermine the benefits of digital transformation.

Future Directions and Emerging Trends

The next decade will see intelligent control systems advance rapidly as emerging technologies mature and industrial, economic, and societal pressures intensify. Several major trends will shape future development: increased autonomy through AI, strengthened cybersecurity, ubiquitous ultra-fast connectivity, expansion of digital twin ecosystems, and alignment with sustainability and human-centric Industry 5.0 principles.

AI-Driven Autonomy and Industry 5.0

As AI and machine learning evolve, control systems will shift from predictive to cognitive and autonomous decision-making. Reinforcement learning and adaptive controllers are expected to manage complex, multi-variable industrial processes with minimal human intervention, enabling flexible manufacturing, self-optimizing plants, and near-zero-downtime operations (Frank et al., 2019). Industry 5.0 emphasizes human–machine collaboration rather than replacement, resulting in workplaces where cobots, AR/VR-enabled interfaces, and AI decision-support tools enhance operator performance and ergonomics (Kagermann et al., 2013; Chang et al., 2021). Workforce development will therefore increasingly require hybrid IT/OT/AI skill sets.

Cybersecurity and System Resilience

Growing connectivity increases exposure to cyber threats. Future architectures will integrate AI-driven intrusion detection, automated isolation mechanisms, and tamper-proof logging—potentially supported by blockchain—to secure device identity and data integrity (Wali & Alshehry, 2024). Standards such as ISA/IEC 62443 and sector-specific compliance frameworks will become central requirements for critical infrastructure (Venanzi et al., 2025). Privacy-preserving analytics (e.g., federated learning) will also gain traction, enabling cloud-scale AI without exposing sensitive operational data.

5G/6G and Ubiquitous Connectivity

5G's ultra-reliable low-latency communication (URLLC) already enables wireless real-time control, mobile robotics, and large-scale IIoT deployments. Future 6G technologies will integrate sensing and communication, allowing devices to share environmental awareness and support distributed fog computing at the network edge (InHand Networks, 2025). Satellite IoT will close remaining connectivity gaps, enabling fully connected supply chains, utilities, and remote industrial assets.

Digital Twin Ecosystems and the Industrial Metaverse

Digital twins are expected to evolve into interconnected networks representing machines, production lines, entire plants, and supply chains simultaneously (Mendonça et al., 2022). These ecosystems will feed into immersive AR/VR environments—sometimes described as the industrial metaverse—enabling remote collaboration, virtual commissioning, advanced maintenance support, and multi-site operational planning (Simio, 2025). As real-time data, simulation models, and AI intersect, digital twins will become continuous optimization engines.

Sustainability and Energy Optimization

Environmental and regulatory pressures will drive more AI-based optimization for energy efficiency and decarbonization. Intelligent control systems will integrate renewable energy variability, minimize emissions, and coordinate production schedules to align with low-carbon electricity availability (Farooq et al., 2023). Industry 5.0 principles reinforce multi-objective optimization, where sustainability metrics carry equal weight to cost or productivity.

Standardization, Convergence, and Unified Architectures

Future progress will depend on greater interoperability. Emerging reference architectures, open standards (OPC UA, MQTT, Digital Twin Definition Language), and open-source industrial

platforms will reduce vendor fragmentation and accelerate deployment (Lu, 2017; Venanzi et al., 2025). Long-term, industries may adopt unified "industrial operating systems" managing IoT, AI, digital twins, and edge–cloud orchestration cohesively.

Overall Outlook

Control systems will become increasingly autonomous, interconnected, resilient, and sustainable. In the long term, quantum optimization—currently experimental—may support complex, national-scale control problems such as grid balancing or large-scale logistics. Achieving these futures will require coordinated innovation across engineering, IT, data science, policy, and education.

Conclusion

The integration of advanced information technologies into technical control systems is reshaping industrial automation and infrastructure management globally. Industry 4.0 has accelerated the convergence of IT and OT, enabling real-time visibility, intelligent decision support, and flexible, data-driven operations across sectors (Frank et al., 2019; Lee et al., 2015). IoT provides continuous data acquisition, cloud and edge computing supply scalable processing and reliable local control, AI introduces predictive and adaptive intelligence, and digital twins offer powerful simulation and optimization capabilities (Chang et al., 2021; Mendonça et al., 2022).

These technologies collectively deliver measurable benefits: reduced downtime, improved product quality, stronger situational awareness, and significant gains in energy and resource efficiency (Farooq et al., 2023; Rustamova & Rustamov, 2024). However, they also introduce challenges—particularly cybersecurity risks, interoperability limitations, and increased architectural complexity. Addressing these issues requires robust security frameworks, adherence to interoperability standards, improved lifecycle management, and substantial workforce upskilling (Wali & Alshehry, 2024; Venanzi et al., 2025).

Looking ahead, intelligent control systems will continue evolving toward higher autonomy, deeper AI integration, pervasive connectivity, and comprehensive digital twin ecosystems. Principles of Industry 5.0—human-centricity, sustainability, and resilience—will increasingly shape system design and operation (Kagermann et al., 2013; Chang et al., 2021). Emerging technologies such as 5G/6G, immersive interfaces, and advanced simulation platforms will further blur boundaries between physical and digital environments.

Ultimately, the fusion of IT and control engineering represents a transformative shift toward smarter, more adaptive, and more sustainable industrial ecosystems. While technical and organizational challenges persist, the trajectory is clear: intelligent, interconnected control systems will become foundational to competitiveness, innovation, and infrastructure resilience in the decades ahead.

References

Chang, Z., Liu, S., Xiong, X., Cai, Z., & Tu, G. (2021). *A survey of recent advances in edge-computing-powered artificial intelligence of things*. IEEE Internet of Things Journal, 8(18), 13849–13875. DOI: 10.1109/JIOT.2021.3088875

Enemosah, A., & Ifeanyi, O. G. (2024). *SCADA in the Era of IoT: Automation, Cloud-driven security, and machine learning applications*. International Journal of Science and Research Archive, 13(1), 3417–3435. DOI: 10.30574/ijsra.2024.13.1.1975

Farooq, M. S., Abdullah, M., Riaz, S., Alvi, A., Rustam, F., López Flores, M. A., Castanedo Galán, J., Samad, M. A., & Ashraf, I. (2023). *A Survey on the Role of Industrial IoT in Manufacturing for Implementation of Smart Industry*. Sensors, 23(21), 8958. DOI: 10.3390/s23218958

Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). *Industry 4.0 technologies: Implementation patterns and their impact on firm performance*. International Journal of Production Economics, 210, 15–26. DOI: 10.1016/j.ijpe.2019.01.004

InHand Networks. (2025, June 13). *Top 10 Industrial IoT Trends in 2025: Empowering the Future of Smart Manufacturing*. Retrieved from InHand Networks Blogs: https://inhandgo.com/blogs/articles/top-10-industrial-iot-trends-in-2025-empowering-the-future-of-smart-manufacturing

Kagermann, H., Wahlster, W., & Helbig, J. (2013). *Recommendations for implementing the strategic initiative INDUSTRIE 4.0*. Final report of the Industrie 4.0 Working Group. acatech – National Academy of Science and Engineering, Germany.

Lee, J., Bagheri, B., & Kao, H. (2015). *A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems*. Manufacturing Letters, 3, 18–23. DOI: 10.1016/j.mfglet.2014.12.001

Lu, Y. (2017). *Industry 4.0: A survey on technologies, applications and open research issues*. Journal of Industrial Information Integration, 6, 1–10. DOI: 10.1016/j.jii.2017.04.005

Mendonça, R. da S., de Oliveira Lins, S., de Bessa, I. V., de Carvalho Ayres Jr, F. A., de Medeiros, R. L. P., & de Lucena Jr, V. F. (2022). *Digital Twin Applications: A survey of recent advances and challenges*. Processes, 10(4), 744. DOI: 10.3390/pr10040744

Moxa. (2021). *6 Challenges for Industrial IoT* (Content published by Moxa, via Madison Technologies). Retrieved from https://madison.tech/6-challenges-for-industrial-iot/

Ness, J. (2025, June 24). *Why Edge Intelligence Is the Future of Industrial Control*. Digi International Blog. Retrieved from https://www.digi.com/blog/post/edge-intelligence-future-of-industrial-control

Rustamova, S., & Rustamov, F. (2024). *Integrating Artificial Intelligence with SCADA Systems: Enhancing Operational Efficiency, Predictive Maintenance, and Environmental Sustainability*. ScienceRise, (2), 106–117. DOI: 10.21303/2313-8416.2024.003691

Simio. (2025, July 17). *Digital Twin Manufacturing: Applications, Benefits, and Industry Insights*. Simio Blog. Retrieved from https://www.simio.com/digital-twin-manufacturing-applications-benefits-and-industry-insights/

Venanzi, R., Di Modica, G., Foschini, L., & Bellavista, P. (2025). *Towards IT/OT integration in industry digitalization: A comprehensive survey*. Journal of Network and Computer Applications, 245, 104373. DOI: 10.1016/j.jnca.2025.104373

Wali, A. M., & Alshehry, F. (2024). *A survey of security challenges in cloud-based SCADA systems*. Computers, 13(4), 97. DOI: 10.3390/computers13040097