Proceedings of the 3rd International Conference on Mechatronics and Smart Systems
DOI: 10.54254/2755-2721/135/2025.21266

Balancing Autonomy and Human Oversight: A Review of Automation and Control Systems in Large-Scale Industrial Processes

Yuxuan Zhou[1,a,*]

[1]*School of Information Sciences, University of Illinois Urbana-Champaign, Illinois, 61820, United States*
a. cabbcab@outlook.com
**corresponding author*

Abstract: Automation and control systems have become indispensable components of modern industrial processes, permeating sectors such as automotive manufacturing, oil and gas production, logistics and warehousing, and countless other domains. As technology advances, questions arise about the optimal degree of automation, the necessary balance between human oversight and autonomous operation, and the most effective approaches to software platforms (open-source versus proprietary). This literature review aims to provide an exploration of automation and control systems within large-scale industrial contexts, illuminating the key debates, pinpointing research gaps, offering concrete examples, and grounding its observations in authoritative references. The discussion centers on what the future holds for industrial automation when considering fully autonomous systems versus hybrid models, along with the trade-offs between open-source software flexibility and proprietary frameworks.

Keywords: Cloud Manufacturing (CMfg), Automation and Control Systems, Artificial Intelligence (AI) Integration, Sustainable Manufacturing, Human-AI Collaboration

1. Introduction

Over the past century, industrial processes have undergone a series of technological transformations, beginning with mechanization and progressing through increasingly complex forms of automation that leverage advancements in electronics, software, and cyber-physical systems [1]. The Industrial Revolution introduced mechanical power to industry, while the twentieth century witnessed the rise of electrical and electronic control mechanisms. From assembly lines pioneered by Ford to highly sophisticated programmable logic controllers introduced later, each incremental leap reduced manual labor in favor of greater consistency and throughput.

In recent decades, the incorporation of computer-based, algorithmically driven systems has given rise to Industry 4.0, a term describing the interconnected, digital manufacturing ecosystem that fuses the physical and cyber worlds [2]. Futuristic visions of "smart factories," wherein machinery can self-monitor, self-diagnose, and collaborate with minimal human intervention, are no longer theoretical concepts; they are steadily becoming a reality in leading sectors such as automotive, semiconductor fabrication, pharmaceuticals, and beyond [3].

DOI: 10.54254/2755-2721/135/2025.21266

Today, the push for energy efficiency, sustainability, and cost-effectiveness has further fueled the popularity of highly automated systems [4]. Moreover, the pandemic underscored the need for resilience and flexibility in manufacturing and supply chain operations, making the topic of automation even more urgent [5]. Consequently, some industries are racing toward fully autonomous solutions, where artificial intelligence (AI) algorithms can adapt and optimize processes, obviating the need for human intervention, barring occasional maintenance or oversight checks. Others, by contrast, emphasize a hybrid model that retains human control over strategic decisions and critical fail-safes.

This literature review addresses these ongoing debates by synthesizing a variety of scholarly and industry sources. The focal question is to investigate the future of automation in large-scale industrial processes, which provides a unifying thread for analyzing the sociotechnical, economic, and ethical considerations that converge in industrial automation decision-making. Key sub-topics include the relative merits of full autonomy versus hybrid oversight, the role of open-source software as opposed to proprietary systems, and the research gaps that continue to limit a more seamless implementation of advanced control systems.

2. Automation and control systems in industrial progress

Automation and control systems encompass a broad range of technologies designed to regulate, monitor, and execute tasks within industrial settings. At their most basic, control systems measure inputs from sensors, compare real-time conditions against desired set points, and provide instructions to actuators or machinery to correct deviations [6]. In more advanced architectures, machine learning algorithms, predictive analytics, and artificial intelligence can analyze vast troves of production data, identify patterns, and optimize processes without requiring step-by-step configurations from human operators [4].

Historically, industrial automation relied on Programmable Logic Controllers (PLCs), which offered programmable sequences for tasks such as conveyor belt operations, painting robots, and assembly arms. Over time, these PLC-based systems were augmented with Supervisory Control and Data Acquisition (SCADA) systems that gather real-time data, feed it to a centralized control room for supervision, and manage all related alarms [7]. The integration of SCADA with distributed control systems (DCS) led to more decentralized decision-making capabilities, wherein each subsystem could operate with partial autonomy [8]. In recent years, Industry 4.0 paradigms have introduced the Industrial Internet of Things (IIoT), enabling “smart devices” on the factory floor to communicate with one another and with cloud-based platforms [9].

The continued integration of AI in manufacturing opens the possibility for “lights-out” factories—facilities that operate entirely without human presence. However, achieving complete lights-out functionality remains challenging because of the unpredictable nature of supply chain variations, mechanical breakdowns, and the complexities inherent in product customization [10]. This push and pull between theoretical possibilities and practical limitations constitutes a central theme throughout this literature.

3. Exist debate

3.1. Fully autonomous systems and Hybrid models

3.1.1. Fully Autonomous Systems Using AI

One of the most significant debates in industrial automation today centers on the benefits and risks of fully autonomous systems, driven by complex AI algorithms, versus hybrid models that retain

DOI: 10.54254/2755-2721/135/2025.21266

substantial human oversight. This debate includes nuanced arguments regarding efficiency, reliability, cost-effectiveness, and ethical considerations.

Advocates of fully autonomous systems often point to the enhanced speed and consistency with which tasks can be executed. AI-driven machines never tire, can run around the clock, and demonstrate remarkable precision in repetitive or hazardous tasks. Autonomous systems also eliminate many common human errors resulting from fatigue or lapses in attention.

Yet, critics caution that full autonomy lacks the human capacity for creativity, improvisation, and empathy [11]. In dynamic industrial environments—such as oil platforms dealing with weather changes, or advanced manufacturing processes requiring frequent reconfiguration—an exclusively AI-driven system may struggle to handle anomalous events that deviate significantly from historical training data. Furthermore, without human oversight, minor system glitches can cascade into catastrophic failures if the AI does not recognize or properly respond to unexpected anomalies [12].

3.1.2. Hybrid Models (Human Oversight Plus AI Integration)

Hybrid systems attempt to resolve these issues by combining AI capabilities in routine or high-speed tasks with specialized human involvement for edge cases, strategic decisions, and safety-critical operations [13]. In such models, humans can oversee system performance, intervene when necessary, and provide nuanced judgment that is difficult to encode into algorithms. Proponents argue that hybrid approaches increase trust in automation technologies among workers and stakeholders. They also provide iterative feedback loops, allowing AI to learn from human input while humans gain insights from AI-generated analytics.

Nevertheless, hybrid models face their own challenges. They can introduce complexities concerning personal accountability, job design, and the risk of over-reliance on automation. An operator supervising many autonomous processes might become complacent, insufficiently attentive to emerging issues, or unprepared to take manual control when the AI signals an anomaly [14]. As a result, the debate focuses on finding the "optimal slice" of autonomy while minimizing skill degradation among the human workforce and ensuring safe, reliable operation.

3.2. OPEN-SOURCE SOFTWARE VS. PROPRIETARY PLATFORMS

3.2.1. Open-Source Software Systems

Parallel to the discussion on autonomy levels is a debate on software ecosystems. Industrial automation systems hinge on software platforms governing everything from sensor calibration to advanced analytics.

Open-source platforms offer transparency, flexibility, cost savings, and a robust, community-driven development infrastructure [15]. Through collaborative efforts, open-source software (OSS) can be rapidly improved and adapted to unique use cases. In the IIoT space, platforms like Eclipse IoT and ThingSpeak provide accessible frameworks for integrating sensors, data streams, and control logic in a highly modular way. This fosters innovation, as teams can tailor solutions to their specific context instead of being constrained by proprietary APIs.

However, open-source software systems may face potential security vulnerabilities when adopters lack rigorous vetting protocols [16]. Without a single responsible entity providing warranties, organizations must rely on community support or build their own technical expertise to address issues. In highly regulated industries—like energy, pharmaceuticals, or defense—this distributed responsibility can deter adoption or raise concerns about liability.

DOI: 10.54254/2755-2721/135/2025.21266

3.2.2. Proprietary Technology Platforms

On the other hand, proprietary solutions often come packaged with warranties, customer support, and robust cybersecurity measures. Market-leading companies such as Siemens, Rockwell Automation, and Schneider Electric provide integrated hardware-software ecosystems with well-documented interfaces and guaranteed performance metrics [8]. These solutions can be advantageous for mission-critical settings where reliability and vendor accountability are paramount. Proprietary platforms are also frequently tested at scale in real industrial environments, conferring a degree of assurance that open-source solutions might not match.

The tension between open-source flexibility and proprietary reliability are central to industrial automation conversations, with many companies attempting a "best of both worlds" approach by integrating open-source libraries within commercial frameworks.

4. Critical research gaps in advanced automation technologies

Notwithstanding the considerable maturity and sophistication of current automation technologies, research gaps persist. Addressing these gaps is essential for progress toward safer, more reliable, and more adaptive control systems.

While numerous studies highlight the potency of AI and autonomous control, data remains sparse on how these systems perform in unforeseen, high-risk scenarios. For example, a manufacturing plant that experiences a sudden supply chain disruption or a hardware malfunction may prompt reactive decisions that AI systems are not prepared to handle, especially when training data does not reflect such extreme cases [12].

Another gap relates to architectural scalability. Many industries—especially oil refineries, power plants, and chemical processing facilities—operate with decades-old infrastructure that cannot be easily replaced. Retrofitting advanced control and automation systems onto legacy frameworks demands an in-depth understanding of system integration and interoperability.[1] Research that provides universal guidelines or standardized protocols for bridging these generations is lacking.

The transition from purely manual to fully automated or hybrid environments introduces complexities in organizational design and workforce training, underscoring the nuanced interactions between humans and automated systems, yet further research is needed to clarify the psychological, managerial, and safety implications when humans serve as supervisory operators [11]. This extends to user interface design, trust calibration, and skill retention—areas critical to long-term viability and safety [13].

Automation systems increasingly rely on networked operations, which expands the attack surface for cyber threats. There is a dearth of comprehensive frameworks addressing real-time anomaly detection, layered defense, and intrusion resilience tailored for industrial control systems (ICS) [17] With the proliferation of IIoT, advanced persistent threats may compromise entire production lines. Research that incorporates robust cybersecurity features within the automation design from the outset, rather than as an afterthought, remains insufficiently explored.

5. Key Frameworks and Safety Considerations for Advanced Automation

Parasuraman, Sheridan, and Wickens' seminal framework conceptualize automation across multiple levels and types, ranging from information acquisition to decision-making and action implementation [11]. Their model underscores the nuance that automation need not be monolithic or absolute; rather, tasks can be parceled out between humans and machines depending on context. Similarly, Lee and See's study on "Trust in Automation: Designing for Appropriate Reliance" investigates how operators develop or lose trust in automated systems based on perceived performance and reliability

DOI: 10.54254/2755-2721/135/2025.21266

[13]. These works ground much of the ongoing discussion regarding how to optimally blend human expertise with machine proficiency.

The "Amazon Robotics Case Study" offers insight into a highly automated warehousing environment. Amazon's fulfillment centers leverage fleets of autonomous robots to move inventory pods within tight, algorithmically optimized corridors. Yet, human workers still handle product picking, quality checks, and packaging, illustrating a pragmatic blend of advanced robotics with localized human decision-making. The success of these centers has spurred further research into swarm robotics, algorithmic route planning, and real-time analytics [18]

High-risk environments such as nuclear facilities, oil rigs, and chemical plants present unique challenges in automation [19]. A single failure can have far-reaching impacts, both financially and for public health and safety. Consequently, control systems in these settings must align with stringent design standards, including redundancy, fail-safe mechanisms, and layers of protection. The integration of advanced AI-based automation must likewise meet rigorous validation protocols [12].

6. Future directions and emerging opportunities

Over the next decade, as industries connect more devices to the Internet, safeguarding these networks from cyber threats will become paramount. Incorporating AI not only for control decisions but also for real-time threat detection may mitigate some of these risks[20] More cross-disciplinary research involving computer security, industrial automation, and systems engineering is needed to robustly protect critical infrastructure.

Another promising area is the development of adaptive learning systems that can dynamically adjust control strategies based on real-time data streams. Current AI models rely heavily on historical data, but as more sensors are introduced and edge computing grows, self-learning industrial systems capable of immediate recalibration could emerge [1]. Harnessing incremental, real-time data for instantaneous decision-making, however, requires breakthroughs not only in machine learning but also in distributed computing, high-bandwidth networking, and robust sensor fusion.

As digital transformation deepens, the role of human operators and technicians seems poised to evolve significantly. Training programs must adapt to cultivate workforce skills in monitoring, AI supervision, data analytics, and emergency intervention [11]. Furthermore, ethical questions about job displacement, responsibility for automated decisions, and the equitable distribution of productivity gains will likely intensify. Researchers across fields—such as industrial-organizational psychology, law, and policy—can contribute to shaping frameworks that ensure fair and transparent deployment of automation.

7. Conclusion

In summary, the evolution of automation and control systems represents a central pillar of modern industrial activities. The thematic lens of what is the future of automation in large-scale industrial processes reveals a landscape shaped by multiple tensions. Chief among them is the dichotomy between fully autonomous AI-driven operations and hybrid configurations that preserve a degree of human involvement. This decision often hinges on risk tolerance, complexity, cost, and the availability of skilled human operators.

Simultaneously, organizations grapple with whether to implement open-source platforms, which promise flexibility but demand considerable in-house expertise, or proprietary systems that provide vendor-backed reliability at the potential expense of interoperability and higher costs. Underlying these debates are pressing research gaps, including insufficient data on system reliability under extreme stress, incomplete frameworks for integration with legacy infrastructures, a limited

DOI: 10.54254/2755-2721/135/2025.21266

exploration into human-machine collaboration dynamics, and the urgent need for robust cybersecurity measures.

Although this literature review examines the application of automation and control systems in large-scale industrial processes, certain limitations exist. For instance, the study primarily focuses on specific industry cases, lacking comparative analysis across various sectors. Additionally, there is insufficient data on system reliability in extreme high-risk scenarios and the development of universal frameworks for integration with legacy infrastructures remains incomplete. Future research should expand cross-industry samples, deeply analyze system adaptability and efficiency in different environments, and develop more robust integration and security mechanisms to advance the optimization and application of automation technologies.

References

[1] *L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, K. Ueda,Cyber-physical systems in manufacturing,CIRP Annals,Volume 65, Issue 2,2016,Pages 621-641,ISSN 0007-8506,https://doi.org/10.1016/j.cirp.2016.06.005.*

[2] *Schwab K. The fourth industrial revolution[M]. Crown Currency, 2017.*

[3] *Lucke D, Constantinescu C, Westkämper E. Smart factory-a step towards the next generation of manufacturing[C]//Manufacturing Systems and Technologies for the New Frontier: The 41 st CIRP Conference on Manufacturing Systems May 26–28, 2008, Tokyo, Japan. Springer London, 2008: 115-118.*

[4] *Jay Lee, Behrad Bagheri, Hung-An Kao,A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems, Manufacturing Letters,Volume 3, 2015, Pages 18-23, ISSN 2213-8463, https://doi.org/10.1016/j.mfglet.2014.12.001.*

[5] *Ivanov D, Das A. Coronavirus (COVID-19/SARS-CoV-2) and supply chain resilience: A research note[J]. International Journal of Integrated Supply Management, 2020, 13(1): 90-102.*

[6] *Ogata K. Modern control engineering[J]. 2020.*

[7] *Bulfone D, Daneels A. International Conference on Accelerator and Large Experimental Physics Control Systems[J]. IEEE Control Systems Magazine, 2000, 20(3): 92-96.*

[8] *McMillan G K, Considine D M. Process/Industrial instruments and controls handbook[M]. New York, NY, USA: McGraw Hill, 1999.*

[9] *Qi Q, Tao F. Digital twin and big data towards smart manufacturing and industry 4.0: 360 degree comparison[J]. Ieee Access, 2018, 6: 3585-3593.*

[10] *Filippo Chiarello, Leonello Trivelli, Andrea Bonaccorsi, Gualtiero Fantoni,Extracting and mapping industry 4.0 technologies using wikipedia,Computers in Industry,Volume 100,2018,Pages244-257,ISSN 0166-3615,https://doi.org/10.1016/j.compind.2018.04.006.*

[11] *Parasuraman R, Sheridan T B, Wickens C D. A model for types and levels of human interaction with automation[J]. IEEE Transactions on systems, man, and cybernetics-Part A: Systems and Humans, 2000, 30(3): 286-297.*

[12] *Leveson N G. Engineering a safer world: systems thinking applied to safety (engineering systems)[J]. MIT Press Cambridge, 2011.*

[13] *Lee J D, See K A. Trust in automation: Designing for appropriate reliance[J]. Human factors, 2004, 46(1): 50-80.*

[14] *Endsley M R, Kiris E O. The out-of-the-loop performance problem and level of control in automation[J]. Human factors, 1995, 37(2): 381-394.*

[15] *Bonaccorsi A, Rossi C. Why open source software can succeed[J]. Research policy, 2003, 32(7): 1243-1258.*

[16] *DiBona C, Ockman S. Open sources: Voices from the open source revolution[M]. " O'Reilly Media, Inc.", 1999.*

[17] *Kushner D. The real story of stuxnet[J]. ieee Spectrum, 2013, 50(3): 48-53.*

[18] *Wurman P R, D'Andrea R, Mountz M. Coordinating hundreds of cooperative, autonomous vehicles in warehouses[J]. AI magazine, 2008, 29(1): 9-9.*

[19] *Reason J. Managing the risks of organizational accidents[M]. Routledge, 2016.*

[20] *Humayed A, Lin J, Li F, et al. Cyber-physical systems security—A survey[J]. IEEE Internet of Things Journal, 2017, 4(6): 1802-1831.*