POSITION PAPER

Industrial AI and Its Impact on Automation

INTRODUCTION

Artificial intelligence (AI) integration in automation and control has evolved from basic rule-based systems to sophisticated, data-driven technologies that drive modern industrial operations. It continues to transform these fields by enabling smarter, more efficient and autonomous systems, paving the way for future innovations in managing and controlling complex processes. As an automation standards and education development organization, ISA is committed to fostering collaboration among stakeholders and promoting the adoption of best practices for safe and reliable AI implementation in industrial environments.

AI IN AUTOMATION

AI has a long history. The Perceptron, the first machine-learning algorithm, was invented in 1943 by Warren McCulloch and Walter Pitts[1] and implemented in hardware by Frank Rosenblatt in 1957. Allen Newell and Herbert Simon's Logic Theorist and General Problem Solver (GPS) programs and Joseph Weizenbaum's ELIZA were also developed in the 1950s and 1960s.[2]

AI has been used in automation since the 1960s, when expert systems were first developed to emulate human decision-making processes.[3] In the 1970s, these expert systems were enhanced to use knowledge bases and inference rules to perform tasks usually requiring human expertise.

Starting in the 1980s, AI techniques like fuzzy logic and neural networks were applied to control systems, improving their adaptability and robustness.[4] This led to developing more sophisticated autonomous systems that could make decisions based on real-time data.

As computational power and data storage increased in the 1990s, AI started to shift from a knowledge-driven approach to a data-driven one. This led to the emergence of machine learning, enabling predictive maintenance and process optimization systems to learn from data and improve their performance over time.[5] The current wave of AI interest is focused on generative AI, systems that create information or predict sequences based on enormous training datasets and vast amounts of compute resources, allowing AI to generalize information and make predictions. Emerging AI architectures, such as neuro-symbolic processing, combine the world of machine learning and earlier

knowledge-based systems. The pursuit of artificial general intelligence, an all-purpose AI that can solve wide ranges of disparate problems, may be only a few years away.

As AI has evolved, it has been utilized to advance and deliver benefits in industrial environments:

- More autonomous and flexible robots, including collaborative robots (cobots), are serving in the manufacturing, healthcare and service industries (with recent advances in vision-language-action models, derived from the generative AI world, offering new ways to control robots).
- The internet of things (IoT) and smart sensors provide vast amounts of data that AI systems analyze to optimize and control processes in real time.
- Deep learning has enabled breakthroughs in image, video and speech recognition, data visualization and trend analysis, which are now used in automated inspection systems, predictive maintenance and quality control.
- Generative AI enables businesses to mine vast quantities of standards, policies and procedures to improve requirements development, compliance assessment and standard operating procedure production.
- AI is being used to develop autonomous vehicles, such as self-driving cars and drones, that could dramatically alter many industries.
- AI is being used to create digital twins, real-time system simulations that can be compared to real-world systems for control, diagnostics and prediction.

CONCERNS OVER AI IN AUTOMATION

The rapid proliferation of AI technologies is leading businesses to incorporate them to achieve business benefits such as reduced cost and improved efficiency. However, implementing AI in industrial environments requires careful consideration due to several critical factors:

- **Human Safety:** Industrial environments involve heavy machinery, hazardous materials and complex processes. AI systems cannot be allowed to malfunction or make unsafe decisions that could affect human safety. Widespread and uncontrolled adoption of AI to automate activities that were previously the province of human experts introduces new vulnerabilities, creating new attack surfaces where automation is used for the first time.
- **System Reliability:** Industrial automation and control systems have high availability and reliability demands. Any AI failure cannot impact these systems, as this can lead to costly downtime, equipment damage or safety incidents.
- **Data Dependency:** AI systems rely on large volumes of data for training and operation. Poor data quality can lead to inaccurate models and suboptimal decision-making, resulting in significant performance or quality issues. For example, AI models for predictive maintenance must accurately predict failures to prevent unexpected outages.
- **Transparency and Explainability:** Machine learning AI systems, especially large models, are essentially black boxes where little, if any, understanding of the performance and behaviors is available, where testing regimes are complex and incomplete, and where the demanding requirements of OT environments create unique challenges for deploying AI. The technology is immature and poorly understood, with no well-established assurance regime and a lack of clear standards.

- **Information Protection and Cybersecurity:** To be effective, AI systems must consume many forms of sensitive information and intellectual property related to processes, products and operations. AI systems are vulnerable to genuinely new forms of attack, including data poisoning, data exfiltration by inference and reconstruction, real-world data poisoning, prompt injection, goal hijacking, universal adversarial triggers, excessive agency and many forms of attack unique to generative AI.

  In addition, open-source AI systems, widely adopted by many organizations, introduce unique cybersecurity issues. Organizations also need to recognize that AI will displace human workers, creating new dangers of insider threats from those being displaced. Careful design and data management are required to ensure data integrity is maintained and sensitive information is not exfiltrated or exploited. AI systems can introduce new cybersecurity vulnerabilities into industrial environments that must be considered in system design and risk assessments.
- **Business Processes:** Introducing AI into industrial processes involves changes in workflows and practices. AI implementations must comply with industry standards, regulations and legal requirements. AI systems are often the result of complex, decentralized projects involving data collection, training runs, system integration and deployment applications, creating complex assurance schemes. AI also affects decision-making transparency. Addressing all these concerns is crucial for successful AI deployment that does not adversely impact industrial operations.
- **Skill Requirements:** Employees will need training to work with AI systems and understand their operational capabilities and limitations. Emerging roles and skills requirements will continue evolving as AI evolves and will require new training. Careful change management underpinning this training is necessary to address employee fears, provide clarity about changes, and ensure a smooth transition.
- **Global Tensions:** AI systems, particularly large generative AI systems, are engineered primarily in the US, creating tensions between where AI is created and where it is globally deployed. Security problems due to the market concentration of AI services in a small number of large corporations create dependencies and single points of failure that represent significant security vulnerabilities.

Careful implementation of AI in industrial environments requires a multidisciplinary approach involving technical expertise, strategic planning and adherence to ethical and legal standards.

CALL TO ACTION

ISA believes that the automation world is uniquely positioned to benefit from the evolution of AI technology, leveraging a robust set of communications, process, safety, security and integration standards that will be needed as the basis of a complete automation ontology to drive data governance and responsible, profitable AI applications.

AI will continue to be adopted as new techniques emerge, computing power increases and new use cases are identified. It is imperative that we work to establish comprehensive standards and enhance educational initiatives to ensure that businesses deploy AI safely and reliably in their operations.

Like other automation technologies, AI will require changes in the workforce, creating new opportunities for professionals who are knowledgeable in AI and automation.

ISA is committed to leading these efforts, fostering collaboration among stakeholders and promoting the widespread adoption of best practices for implementing AI in industrial environments.

We call on industry leaders, policymakers and academic institutions to join us in this mission. By working together, we can develop the necessary standards, provide valuable education and training, and drive the adoption of AI to benefit society as a whole.

WHERE TO START

As a nonprofit, international professional association, ISA develops widely used safety, security and performance standards for automation. ISA is the primary developer of a series of international consensus standards addressing the security of industrial automation and control systems. The ISA/IEC 62443 standards provide a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in those systems. These are among numerous ISA standards and guidelines that support manufacturing and supply chain efficiency and safety.

ISA actively supports global efforts to establish training and competency programs as part of its commitment to educating and certifying automation professionals. An example is the Automation Competency Model developed by the US Department of Labor. This model defines the key skills, knowledge and abilities that automation professionals need at every career level, from entry-level to advanced. Recognizing that the automation profession is constantly evolving, the model is updated regularly to ensure that emerging technologies are included.

ABOUT ISA

The International Society of Automation (ISA) is a nonprofit professional association founded in 1945 to create a better world through automation. ISA empowers the global automation community through standards and knowledge sharing, driving the advancement of individual careers and the overall profession. ISA develops widely used global standards; certifies professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its members and customers around the world.

RESOURCES

isa.org/standards	138+ standards for automation, cybersecurity and more
isa.org/training	Unbiased, real-world training courses, personnel certifications and certificates that help engineers and technicians take the next step in their automation career
isa.org/join	Membership in ISA offers unparalleled access to technical discussions and resources
isa.org/events	Network, hear best practices and be part of the automation community dialogue at ISA events

WORKS CITED

[1] W. S. McCulloch, and W. Pitts, "A logical calculus of the ideas immanent in nervous activity," Bulletin of Mathematical Biophysics 5 (1943): 115–133, https://doi.org/10.1007/BF02478259.

[2] M. Choubey, "A brief history of AI," Tech Tonic (31 January 2024), retrieved 8 January 2025, https://medium.com/deno-the-complete-reference/a-brief-history-of-ai-0d495513f5c3.

[3] G. Press, "History Of AI In 33 Breakthroughs: The First Expert System," Forbes, (29 October 2022), retrieved 8 January 2025, https://www.forbes.com/sites/gilpress/2022/10/29/history-of-ai-in-33-breakthroughs-the-first-expert-system/.

[4] S. Roberts, "Remembering Lotfi Zadeh, the Inventor of Fuzzy Logic," The New Yorker, retrieved 8 January 2025, https://www.newyorker.com/tech/annals-of-technology/remembering-lotfi-zadeh-the-inventor-of-fuzzy-logic.

[5] G. Fircan, "The History of Machine Learning," retrieved 8 January 2025, https://www.lightsondata.com/the-history-of-machine-learning/.