POSITION PAPER

Automation Shapes Global Economic Growth and Development

INTRODUCTION

Automation has long played a major role in addressing the needs of developed and developing economies by providing multiple benefits in the production and distribution of goods and services — including increased productivity, cost reductions, improved quality, enhanced safety and greater reliability. Moreover, automation technologies have reduced human workloads, transformed labor markets and increased access to goods and services while reducing environmental impacts across all sectors of industry and infrastructure.

POSITION

In the coming years, there is no doubt that automation will continue to provide these many benefits, as it is increasingly applied to enhance such areas as supply chain resilience and global energy efficiency and sustainability. At the same time, however, the automation profession will require skilled and experienced engineers and other professionals, as it repurposes existing jobs, creates new ones and balances workforce skills shortages by enabling greater productivity.

The International Society of Automation (ISA) — a nonprofit global association of automation engineers and specialists — is committed to being the "home of automation," responding to the needs of society and industry and supporting the profession and practice of the automation discipline.

OUTLOOK FOR AUTOMATION

Against this backdrop, ISA offers this outlook on some of the key areas in which automation will continue to shape the future.

SUPPORTING SUPPLY CHAIN RESILIENCY

The global pandemic and political instability have forced many manufacturers to shift their operations closer to home as they seek to increase efficiencies and reduce supply chain risks. ISA believes manufacturers can optimize their efforts to adapt and strengthen their supply chains by:

- Adopting flexible manufacturing principles to allow for more dynamic responses to changes in production demands, raw material availability and ongoing shortages of skilled labor, providing greater resilience during periods of crisis.
- Embracing the wider use of technologies — such as the internet of things, robotics, blockchain and artificial intelligence — in their automation strategies to mitigate differences in costs from onshore to offshore, while increasing accuracy, visibility and customer satisfaction.
- Recognizing and following industry standards that advance interoperability, quality assurance and safety throughout the supply chain.
- Adopting industrial automation and control systems cybersecurity standards and conformity assessment programs to protect their operations against operational impacts from intentional and unintentional incidents — and to protect their intellectual property.
- Applying automation to improve the efficiency of warehouses and order fulfillment. Robots can pick and pack orders, which helps reduce the amount of time and energy required for fulfillment.
- Applying automation and process control in support of the many of the steps involved in vehicle manufacturing and assembly, helping reduce the amount of pollution produced by the manufacturing process.
- Using automation-based solutions to reduce and sort waste. For example, on-site robots can sort and recycle materials, which has helped reduce the amount of waste that goes to landfills.

SUPPORTING ENERGY EFFICIENCY AND SUSTAINABILITY

Safe and efficient execution of the energy production, storage and transmission systems the world depends on requires proven automation technologies implemented by knowledgeable and skilled automation professionals. ISA believes the following automation-based approaches will be essential in the energy sectors:

- Smart grid technologies, incorporating digital communication and control technologies to optimize energy distribution, monitor grid conditions in real time and accommodate variable renewable energy inputs.
- Demand-response programs that adjust electricity consumption based on supply conditions, helping manage peak demand and reduce strain on power grids.
- Recognizing and following industry standards that facilitate interoperability and enhance safety throughout power grids.
- Adopting industrial automation and control systems cybersecurity standards and conformity assessment programs to protect energy production, storage and transmission systems against operational impacts from intentional and unintentional incidents.

ADVANCING CYBERSECURITY RESILIENCY

The impacts of cyber intrusions on banking, business and government networks and databases have been widely publicized and are well known to the public. Much less publicized and understood are the devastating impacts to public safety and welfare that could result from cyberattacks on the networks and technology that underlie the vast critical infrastructure and manufacturing sectors on which all modern economies depend. Compromise — whether malicious or unintentional — could result in any or all of the following:

- Harm to public and/or employees
- Loss of critical infrastructure services including power grids and water processing
- Damage to critical operational machinery
- Major economic losses
- Loss of proprietary or confidential information
- Violation of regulatory requirements
- Harm to the natural environment

ISA believes critical infrastructure and manufacturing sectors should work to enhance their cybersecurity resiliency and reduce their risks by:

- Enacting a cultural shift that prioritizes cybersecurity alongside functionality, efficiency and safety as one of the fundamental workplace tenets in training their workforce.
- Adopting international consensus standards addressing the security of industrial automation and control systems. The ISA/IEC 62443 series of standards provides a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in those systems.
- Requiring vendors to provide products and systems that are secure by design. ISA offers the leading conformity assessment program for industrial cybersecurity products and systems — ISASecure® — which certifies against the ISA/IEC 62443 series of standards.
- Following guidance from the ISA Global Cybersecurity Alliance (ISAGCA), which advances cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes.

ENHANCING THE MODERN WORKFORCE

ISA believes it is vital for governments and other decision makers at all levels to understand the full impact and benefits of automation when assessing its value and use in specific applications — recognizing that automation can be employed to help meet many critical needs and objectives, including:

- Helping perform jobs that cannot be filled in the labor shortages that some industries are experiencing.
- Helping produce vital goods such as pharmaceuticals at lower costs, making those goods more affordable for people who depend on them.
- Helping make goods such as foods and beverages safer for human consumption — and at lower costs.
- Helping protect or even remove humans from dangerous work and situations, such as in law enforcement, search and recovery, harsh and hazardous manufacturing operations and the like.
- Freeing resources from performing mundane and repetitive tasks, allowing them to be directed to other, more challenging and rewarding activities.

RECOMMENDATIONS

Decision makers — including those in industry, government and academia — can help deliver the many benefits of automation more effectively in several essential ways, including:

- Supporting the ongoing development of industry standards addressing key aspects of people, processes and technology in automation systems.

- Encouraging educational institutions to increase the availability of degree programs, courses and training aligned to prepare future automation professionals.
- Supporting the adoption of certification and certificate programs to strengthen the skills and knowledge of the automation professionals we all depend on.

ISA recommends that governments looking to secure their critical infrastructure should:

- Encourage their manufacturing and critical infrastructure sectors to adopt the ISA/IEC 62443[1] series of consensus standards addressing the security of industrial automation and control systems.
- Direct their regulations toward ensuring that critical infrastructure owner-operators apply a formal risk-based approach to cybersecurity management.

ISA further recommends that organizations looking to secure their critical infrastructures should:

- Support their front-line engineers by fostering a cybersecurity culture within their organizations, which prioritizes cybersecurity alongside other fundamental workplace tenets like efficiency and safety.
- Provide ample opportunities for engineers to be trained and certified on the specific requirements of cybersecurity of industrial automation and control systems.

WHAT ISA OFFERS

As a nonprofit international professional association, ISA develops widely used safety and performance standards for automation; provides education, training and certification programs for automation professionals; publishes books and technical articles; and provides networking and career development programs for automation professionals worldwide.

ISA is the primary developer of a widely used 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 standards are among numerous ISA standards and guidelines that support manufacturing and supply chain efficiency and safety.

ISA created the ISA Global Cybersecurity Alliance (ISAGCA)[2] to advance cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes. The Alliance brings end-user companies, automation and control systems providers, IT infrastructure providers, services providers, system integrators and other cybersecurity stakeholder organizations together to proactively address growing threats. ISA also offers the leading conformity assessment program for industrial cybersecurity products and systems — ISASecure[3] — which certifies against the ISA/IEC 62443 series of standards.

As part of its commitment to the education and certification of automation professionals, ISA actively supports global efforts to establish training and competency programs. An example is the Automation Competency Model[4] developed by the US Department of Labor. This model defines the key skills, knowledge and abilities that automation professionals need from entry level to advanced career level. It is updated regularly to ensure emerging technologies are included, recognizing that the automation profession is constantly evolving.

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] ISA. (n.d.). ISA/IEC 62443 Series of Standards. Retrieved July 14, 2023, from https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards/

[2] ISA. (n.d.). ISA Global Cybersecurity Alliance. Retrieved July 14, 2023, from https://www.isagca.org/

[3] ISA Security Compliance Institute. (n.d.). Home. Retrieved July 14, 2023, from https://www.isasecure.org/

[4] Automation Competency Model. (2018). US Department of Labor. Retrieved from https://www.careeronestop.org/competencymodel/competency-models/automation.aspx