Enhancing Process Efficiency and Security in the U.S. Manufacturing Sector: Evidence from Industry Implementation

AYOKUNLE AKINSANYA
Management Information Systems Department, Bowie State University

Abstract *- The U.S. manufacturing sector is at a critical juncture, facing the dual challenges of maintaining global competitiveness and addressing escalating cybersecurity threats. As Industry 4.0 technologies such as the Internet of Things (IoT), artificial intelligence (AI), and advanced robotics redefine production processes, manufacturers must simultaneously optimize operational efficiency and fortify their digital infrastructure. Drawing from systematic review of industry developments between 2019-2024 and real-world implementations, including detailed case studies, this article presents a holistic framework for achieving these objectives, integrating cutting-edge technological innovations, workforce development, and robust cybersecurity measures. Analysis of industry implementations demonstrates significant improvements, including 30-50% reductions in operational inefficiencies, 80% decrease in security incidents, and 4-5% annual productivity gains through digital transformation. By adopting a multidisciplinary approach, manufacturers can not only enhance productivity but also build resilience against emerging threats. This work provides practical, evidence-based strategies for manufacturing leaders, contributing to the growing body of literature on smart manufacturing and industrial cybersecurity while offering actionable insights for practitioners and policymakers.*

Indexed Terms- *Digital Transformation, Industry 4.0, Industrial Cybersecurity, Process Efficiency, Smart Manufacturing*

I. INTRODUCTION

The U.S. manufacturing sector remains a vital component of the national economy, contributing approximately $2.93 trillion to GDP and employing over 13 million workers [18]. However, the sector is undergoing a profound transformation driven by the Fourth Industrial Revolution, characterized by the convergence of digital, physical, and biological systems. While these advancements present unprecedented opportunities for efficiency gains, they also introduce complex vulnerabilities, particularly in cybersecurity. The IBM X-force report shared by Infosecurity magazine, manufacturing was the most targeted industry for cyberattacks, accounting for 25.7% of all incidents observed in 2023 [12].

The convergence of digital technologies in manufacturing environments has created both opportunities and vulnerabilities. As factories become increasingly connected and automated, the distinction between physical and digital operations continues to blur, creating new paradigms for production and control. This digital transformation, while essential for maintaining competitive advantage, requires careful consideration of security implications.

II. METHODOLOGY

This research employed a systematic review methodology to examine the intersection of manufacturing efficiency and cybersecurity in the U.S. manufacturing sector. The review focused on literature and industry developments from 2019-2024, encompassing both academic publications and industry reports.

Research Protocol

- Literature sources: Academic journals, industry reports, technical standards, and case studies
- Focus areas: Smart manufacturing, process efficiency, cybersecurity, and Industry 4.0

- Analysis approach: Synthesis of findings across sources to identify patterns, best practices, and implementation frameworks

Analysis Framework

- Content analysis of key themes in efficiency and security integration
- Framework development based on identified best practices
- Validation through case study analysis and industry standards comparison

This methodology enabled comprehensive examination of how manufacturers can optimize efficiency while maintaining security measures.

III. INDUSTRY CONTEXT AND ANALYSIS

The Imperative for Process Efficiency in Manufacturing

The pursuit of process efficiency has become a critical imperative for the U.S. manufacturing sector in the face of increasing global competition and rapid technological advancements. Manufacturers are embracing strategies such as smart manufacturing, automation, robotics, and lean principles to optimize operations, reduce waste, and boost productivity. The integration of these approaches with digital technologies is transforming production processes and enabling manufacturers to achieve new levels of efficiency. As the sector navigates this complex landscape, the focus on process efficiency is crucial for maintaining competitiveness, driving growth, and building resilience.

3.1. Smart Manufacturing and Industry 4.0

Smart manufacturing, a cornerstone of Industry 4.0, encompasses the integration of advanced production systems with digital technologies, including sensor networks, computational infrastructure, and data-driven modeling capabilities for enhanced control and predictive operations [14].

Manufacturing has evolved into an intelligent ecosystem where digital technologies converge. This modern approach combines networked systems, cloud-based operations, and data analytics with AI-driven decision making to create an interconnected production environment [17]. This transformation represents a fundamental change in manufacturing operations, where sensor-equipped machinery continuously gathers operational data, allowing companies to spot production bottlenecks and make timely adjustments to enhance efficiency. AI and machine learning algorithms further enhance decision-making by predicting equipment failures, optimizing supply chains, and reducing energy consumption [16]. These technologies not only improve operational efficiency but also enable manufacturers to respond swiftly to changing market demands.

3.2. Automation and Robotics: Redefining Production

Automation has long been a cornerstone of manufacturing efficiency, but recent advancements in robotics have expanded its potential. Collaborative robots (cobots), equipped with advanced sensors and AI capabilities, are increasingly being deployed to perform repetitive tasks with precision, helping workers in their assigned tasks and improve the results and work conditions by combining workers' skills and robots' physical strength and endurance [13]. Additionally, Autonomous Mobile Robots (AMRs) have emerged as a transformative force in manufacturing and logistics operations. These robots leverage sophisticated decision-making algorithms to navigate independently through complex industrial environments, performing material handling tasks with remarkable efficiency [11]. Their advanced control systems enable them to not only move safely among human workers but also adapt to changing conditions in real-time, making them invaluable for dynamic manufacturing settings. The integration of object recognition and manipulation capabilities further enhances their utility, allowing them to interact meaningfully with their environment while maintaining operational safety through decentralized navigation protocols.

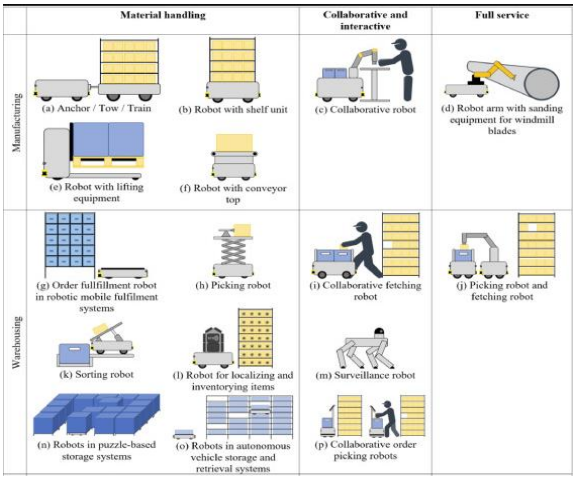

Fig 1: Collaborative Robot

3.3. Lean Manufacturing and Continuous Improvement

Lean manufacturing principles, which originated from the Toyota Production System, continue to play a vital role in modern manufacturing excellence. This methodology focuses on waste reduction and resource optimization throughout the production lifecycle, from design to manufacturing, while maintaining high quality standards and employee engagement [15]. As manufacturing enters the digital age, the convergence of lean principles with Industry 4.0 technologies has created new opportunities for operational excellence. This integration, often termed "digital lean," combines traditional waste reduction methods with advanced digital technologies to enhance productivity and flexibility through decentralized control systems [6]. The synergy between lean methodologies and Industry 4.0 capabilities enables manufacturers to achieve greater efficiency while maintaining the fundamental principles of continuous improvement and waste elimination.

3.4.Digital Transformation in Practice

The theoretical frameworks discussed previously find compelling validation in recent industry implementations. A notable example comes from Rockwell Automation's comprehensive digital transformation across twenty global manufacturing facilities [22]. Their systematic approach to digital integration demonstrates how theoretical concepts translate into measurable operational improvements in modern manufacturing environments.

3.4.1 Infrastructure Integration and Results

Rockwell Automation's transformation began with the fundamental integration of multiple disparate systems into a unified enterprise resource planning (ERP) system. This was complemented by implementing a manufacturing execution system (MES) as their centralized system of record, establishing the foundation for comprehensive digital operations [22].

This systematic approach yielded significant measurable outcomes:

- 4-5% annual improvement in productivity
- Reduction in inventory days from 120 to 82
- 30% capture in annual capital avoidance
- Improvement in supply chain deliveries to 96%
- 50% reduction in lead times

These results validate the effectiveness of integrated digital approaches in modern manufacturing environments and provide concrete benchmarks for industry transformation initiatives.

IV. SECURITY CONSIDERATIONS OF THE GROWING CYBER THREAT LANDSCAPE IN MANUFACTURING

The manufacturing sector faces a growing cybersecurity threat landscape as the increasing integration of technology, from Industrial Control Systems (ICS) to the Internet of Things (IoT), introduces new vulnerabilities. Cyberattacks can disrupt production, compromise sensitive data, and even threaten national security. This section will explore the evolving nature of these threats, including the role of human factors and the importance of adopting a zero-trust security model.

4.1. Vulnerabilities in Industrial Control Systems (ICS)

Industrial control systems, which govern critical manufacturing processes, are increasingly targeted by cybercriminals. These systems, often legacy infrastructure, were not designed with cybersecurity in mind, making them susceptible to attacks such as ransomware and distributed denial-of-service (DDoS) attacks. The 2021 Colonial Pipeline attack, which disrupted fuel supplies across the U.S., underscores the devastating consequences of such breaches [23].

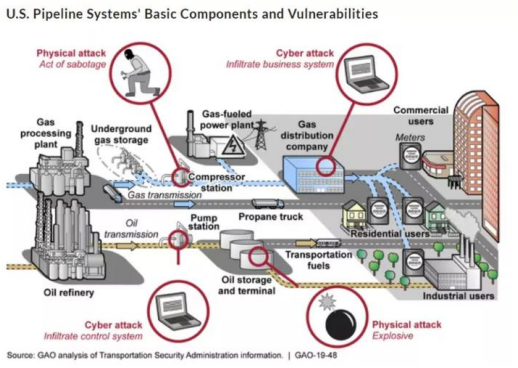

Fig 2: GAO Analysis of Vulnerabilities in ICS

Traditional detection techniques face difficulties due to the increasing complexity and interconnectedness of critical infrastructure systems. Although there are efforts to expand IDS/IPS capabilities from IT into OT networks, threat detection is severely hampered by the lack of standardized protocols and interfaces for physical components [21]. The proprietary nature of these systems and absence of established communication protocols further complicates secure design and operation. An industry consortium called O-PAS (Open Process Automation Standard) aims to create a set of open, collaborative standards on communication protocols and security postures, intending to standardize the diverse array of proprietary CPS [4].

The proliferation of IoT devices within industrial settings has significantly increased cyber vulnerabilities, particularly within critical infrastructure sectors such as electricity grids and water distribution systems. These cyberattacks pose a severe threat, aiming to disrupt essential operations and potentially leading to widespread chaos and a significant decline in a nation's ability to respond to emergencies [2]. Furthermore, the financial impact of data breaches remains substantial, with the average cost in the United States reaching $9.48 million in 2023 [2]. This escalating threat landscape is characterized by a diverse range of actors, including cybercriminals, nation-states, and transnational criminal organizations, who employ sophisticated and malicious tactics to steal intellectual property, conduct espionage, compromise critical infrastructure, and undermine democratic institutions.

4.2. Human Factors in Cybersecurity

The U.S. manufacturing sector is undergoing a digital transformation, leveraging technologies such as the Industrial Internet of Things (IIoT), automation, and cloud computing to enhance efficiency and sustainability. However, this shift has also introduced significant cybersecurity challenges. While technological solutions like firewalls and encryption are essential, human factors play a critical role in either strengthening or undermining cybersecurity efforts.

4.2.1 The Human Element in Cybersecurity

The human element remains a critical vulnerability in manufacturing cybersecurity, accounting for 74% of total breaches across industries according to Verizon's 2023 Data Breach Investigations Report [24]. In the manufacturing sector, where operational technology (OT) and information technology (IT) systems are increasingly interconnected, human-related vulnerabilities become particularly concerning. The report highlights how social engineering attacks, especially phishing, continue to exploit human behavior by manipulating users into clicking malicious links or attachments. This vulnerability is further complicated by issues such as weak password practices and system misconfiguration errors.

1. Employee Awareness and Training:

Employee awareness and training serve as the foundation of manufacturing cybersecurity defense, where both operational technology (OT) and information technology (IT) systems intersect. According to research, 72% and 95% of cyber threats originate from employees' naive security practices, highlighting why organizations must implement comprehensive Security Education Training and Awareness (SETA) programs [9]. These initiatives should address both prevention and countermeasures, using real-world scenarios to demonstrate potential threats while fostering a culture of shared responsibility for cybersecurity across all organizational levels.

2. Organizational Culture and Leadership

Leadership plays a fundamental role in establishing and maintaining a robust cybersecurity culture within manufacturing organizations. According to Deloitte's study on cyber risk in advanced manufacturing, effective cybersecurity requires top-down

commitment where leadership actively promotes security awareness through organization-wide engagement and creates incentives that make every employee responsible for the organization's security posture [10]. This cultural transformation is achieved through measurable cybersecurity learning programs that reshape corporate values and daily employee behaviors. By fostering a security-minded culture, organizations can better protect their complex technological infrastructure, which typically includes global networks, business applications, industrial control systems, and embedded technologies, from increasingly sophisticated cyber threats [10].

4.3. Zero-Trust Architecture

The U.S. manufacturing sector faces a pressing need to adopt a Zero-Trust Architecture to bolster its cybersecurity posture and safeguard critical processes. Traditional perimeter-based security models are no longer sufficient in the era of increased digitization, remote work, and interconnected systems. The Zero-Trust approach rejects implicit trust and instead mandates continuous verification and strict access controls for all users, devices, and applications [2]. By implementing key components such as multifactor authentication, micro-segmentation, and identity and access management, manufacturing organizations can significantly reduce the risk of breaches caused by compromised credentials or malicious insiders [2]. Embracing the Zero-Trust model is crucial for the sector to enhance process efficiency, protect sensitive data, and maintain resilience in the face of evolving cyber threats. Adopting this comprehensive security framework will enable U.S. manufacturers to drive sustainable growth while mitigating the disruptive impact of potential cyberattacks.

V. INTEGRATION FRAMEWORK

5.1. Operational Technology (OT) and Information Technology (IT) Convergence

The convergence of Operational Technology (OT) and Information Technology (IT) represents a transformative approach in modern manufacturing, fundamentally reshaping how industries manage and optimize their production processes. Manufacturing enterprises increasingly recognize that successful digital transformation requires seamless integration between operational systems and information infrastructure, driving the development of sophisticated integration frameworks [7].

5.1.1 Historical Context and Implementation

Traditional manufacturing environments maintained strict separation between OT and IT domains, primarily due to distinct operational requirements and security considerations. However, the emergence of Industrial Internet of Things (IIoT) has catalyzed a shift toward integrated frameworks that bridge this historical divide. These frameworks facilitate real-time data exchange, enhance monitoring capabilities, and improved decision-making processes across manufacturing operations [20].

5.1.2 Cybersecurity Integration Considerations

As OT and IT converge, cybersecurity becomes a critical component of the integration framework. The National Institute of Standards and Technology (NIST) Manufacturing Profile emphasizes the importance of integrating cybersecurity considerations throughout the manufacturing system development lifecycle [19]. This approach involves incorporating security requirements into every phase of design, implementation, and testing, with the goal of reducing potential vulnerabilities.

Key cybersecurity strategies for OT/IT convergence include:

1. *Access Control and Network Segmentation:* Organizations must implement robust access control mechanisms and network segmentation. This can involve maintaining separate networks with carefully controlled interconnections or implementing partial integration through strategic network partitioning [8]. The goal is to protect network integrity while enabling necessary communication between OT and IT systems.
2. *Anomaly Detection and Incident Response:* With increased system integration, developing advanced detection and response capabilities becomes crucial. This involves establishing baselines of network operations, detecting and analyzing anomalous activities, and maintaining comprehensive incident response plans [19].

The implementation of integration frameworks typically progresses through distinct developmental

phases, beginning with organizational alignment. This crucial initial stage focuses on harmonizing workflows between IT and OT teams, establishing shared protocols, and developing unified operational procedures. The technical implementation phase follows where organizations design and deploy the actual convergence architecture, incorporating essential security measures and validation protocols [7].

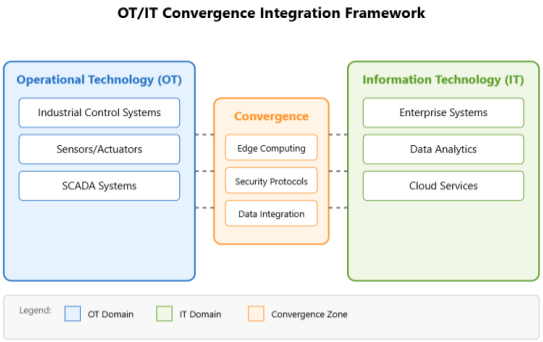

Fig 3: OT/IT Convergence

- *Modern Integration Approaches*

Modern integration frameworks emphasize flexibility in deployment approaches, recognizing that different manufacturing environments require tailored solutions. Some organizations opt for maintaining separate networks with controlled interconnections, while others implement partial integration through network partitioning. Advanced implementations might pursue full integration, incorporating OT traffic directly into IT infrastructure, though this approach demands rigorous security measures and careful consideration of operational requirements.

The evolution of edge computing has introduced new possibilities in OT/IT convergence frameworks. Edge-enhanced architecture enables localized processing and data management, reducing latency and improving operational reliability. This distributed approach allows manufacturing facilities to process critical data closer to production equipment while maintaining connectivity with broader enterprise systems [20].

- *Standards and Implementation Considerations*

Standardization efforts, particularly through protocols like OPC Unified Architecture, have significantly influenced framework development. These standards provide essential guidelines for achieving interoperability across diverse manufacturing systems while maintaining operational integrity. The emergence of publishing/subscribe communication models has further enhanced framework flexibility, enabling more dynamic and scalable integration solutions.

Integration frameworks must address several critical aspects simultaneously: operational efficiency, system security, data integrity, and process reliability. Successful implementations demonstrate measurable improvements in manufacturing performance, including reduced maintenance costs, enhanced production consistency, and improved operational visibility [7].

- *Industrial Impact and Future Directions*

The industrial sector continues to benefit from these advanced integration frameworks, particularly in areas requiring precise control and monitoring. Remote management capabilities, enabled by robust OT/IT integration, allow organizations to optimize operations while maintaining high safety and reliability standards. This convergence supports proactive maintenance strategies and enables more efficient resource allocation across manufacturing operations.

Looking ahead, integration frameworks will likely continue evolving, incorporating new technologies and addressing emerging industrial requirements. The focus remains on creating resilient, secure, and efficient manufacturing environments that can adapt to changing market demands while maintaining operational excellence.

5.2. Data-Driven Decision-Making and Predictive Analytics

Enhancing process efficiency and security in the U.S. manufacturing sector requires a comprehensive framework that leverages data-driven decision-making (DDD) and predictive analytics to drive sustainable growth and resilience. The rise of these approaches has transformed industry, enabling organizations to capitalize on vast troves of information for strategic advantage.

Early adopters of DDD practices achieved productivity gains of 4-8% compared to non-adopters,

with the most significant benefits realized from 2005-2010 [5]. By 2015, 76% of manufacturers used predictive analytics to enable proactive decision-making and enhanced forecasting capabilities [5].

Notably, firms that invested in robust IT infrastructure before implementing DDD saw greater improvements than those that added IT capabilities later [5]. This highlights the importance of strategic sequencing in digital transformation initiatives, particularly in the context of enhancing process efficiency and security.

The key takeaway is that manufacturers aiming to optimize their processes and bolster security should strategically implement DDD and analytics, considering timing and IT infrastructure needs. Staying competitive and resilient in today's rapidly evolving landscape requires continually advancing data capabilities and analytical sophistication. Manufacturers that successfully navigate this transition will be well-positioned to unlock new levels of efficiency, productivity, and security, ultimately fostering sustainable growth in the face of ever-changing challenges.

5. 3. Collaboration and Knowledge Sharing

Manufacturing organizations thrive on effective knowledge sharing and collaborative practices. Research demonstrates that strong inter-organizational relationships significantly enhance knowledge creation and innovation potential in manufacturing environments [1]. When organizations foster environments of trust and open communication, they establish robust foundations for improved performance and security protocols.

Recent industry implementations provide compelling evidence of these principles in action. Rockwell Automation's approach to knowledge management illustrates effective scaling of collaboration across global operations. Their implementation of AR-guided training systems during a plant relocation between Switzerland and Poland achieved notable results - creating 80 detailed instructional videos within a day and reducing training time by 30% through AR-guided systems [22]. This practical application validates research findings that organizational relationships and supportive environments significantly impact knowledge creation capabilities [1].

The successful integration of collaborative frameworks with advanced technologies demonstrates how manufacturing organizations can build more resilient operations while maintaining efficiency in knowledge transfer and security protocols.

5.4 Advanced Manufacturing Systems Integration

Recent industry implementations validate the theoretical benefits of integrated manufacturing systems. Rockwell Automation's deployment of FactoryTalk Innovation Suite across six global facilities exemplifies successful integration of advanced technologies, including:

- Edge-to-enterprise analytics
- Machine learning applications
- Internet of Things (IoT) implementation
- Augmented reality (AR) integration

This comprehensive integration made data more accessible, enabled more informed business decisions, and facilitated long-term growth and continuous innovation [22].

5.4.1 Implementation Outcomes

The results of this system’s integration were significant and measurable:

- 33% increase in labor efficiency at pilot facilities
- 70% increase in output
- 50% reduction in training time
- 8% improvement in productivity through IoT implementation

This practical implementation demonstrates how theoretical frameworks for integrated manufacturing systems can drive substantial operational improvements while maintaining security and efficiency [22].

VI. CONCLUSION AND FUTURE DIRECTIONS

The U.S. manufacturing sector must fundamentally transform its approach to process efficiency and cybersecurity in response to escalating digital threats and competitive pressures. This analysis demonstrates

that manufacturers achieving sustainable growth are those implementing integrated frameworks that address both operational excellence and security resilience.

Industry evidence validates this dual focus. Organizations adopting comprehensive digital transformation strategies have documented substantial improvements: 4-5% annual productivity gains, 80% reduction in quality-related recalls, and 30% avoidance through enhanced operational efficiency. The Rockwell Automation implementation particularly illustrates how strategic technology integration can drive measurable performance improvements while strengthening security postures.

Critical areas requiring future research attention include:

1. Quantum-Safe Security: As quantum computing capabilities advance, research must explore secure communication protocols and encryption methods that protect manufacturing systems against emerging quantum threats.
2. Edge Computing Security: With increased deployment of edge devices in manufacturing environments, investigation of secure edge computing architectures becomes essential for maintaining both efficiency and protection.
3. AI-Enhanced Security Operations: Further research should examine how artificial intelligence can strengthen threat detection while optimizing manufacturing processes, particularly in OT/IT convergence scenarios.

Policy implications are significant. Manufacturing leaders and policymakers must:

- Develop standards that support innovation while ensuring security
- Create incentives for implementing comprehensive security measures
- Foster collaboration between public and private sectors
- Support workforce development in both technical and security domains

Success in modern manufacturing requires strategic balance between operational innovation and security resilience. Organizations mastering this integration will be best positioned to thrive in an increasingly complex digital manufacturing landscape.

REFERENCES

[1] Abubakar, A. M., Elrehail, H., Alatailat, M. A., & Elçi, A. (2019). Knowledge management, decision-making style and organizational performance. Journal of Innovation & Knowledge, 4(2), 104-114. https://doi.org/10.1016/j.jik.2017.07.003

[2] Akinsanya, A. (2024). Securing the Future: Implementing a Zero-Trust Framework in U.S. Critical Infrastructure Cybersecurity. International Journal of Advance Research, Ideas and Innovations in Technology, 10(3), 193-202. 10.5281/zenodo.12550764

[3] Aminu, M., Akinsanya, A., Oyedokun, O., & Akinwande, O. T. (2024). A Review of Advanced Cyber Threat Detection Techniques in Critical Infrastructure: Evolution, Current State, and Future Directions. International Journal of Computer Applications Technology and Research, 13(8), 74-87.

[4] Bartusiak, R. D., Bitar, S., Debari, D., Houk, B., Heaton, M., Strebel, R., Stevens, D., Fitzpatrick, B., & Sloan, P. (2022). Open Process Automation: A standards-based, open, secure, interoperable process control architecture, Control Engineering Practice https://doi.org/10.1016/j.conengprac.2021.105034

[5] Brynjolfsson, E., & McElheran, K. (2019). Data in action: Data-driven decision making and predictive analytics in U.S. manufacturing. Rotman School of Management Working Paper No. 3422397, http://dx.doi.org/10.2139/ssrn.3422397

[6] Buer, S.-V., Strandhagen, J. O., & Chan, F. T. S. (2018). The link between Industry 4.0 and lean manufacturing: Mapping current research and establishing a research agenda. *International Journal of Production Research, 56*(8), 2924-2940. https://doi.org/10.1080/00207543.2018.1442945

[7] Chaiyasoonthorn, S., Wiboonrat, M., Mitatha, S., Sriudomsilp, T., & Siripongdee, S. The Information Technology (IT) and Operational Technology (OT) Convergence in Industrial World.

[8] Cybersecurity and Infrastructure Security Agency. (2020). Critical manufacturing cybersecurity framework implementation guidance. https://www.cisa.gov/resources-tools/resources/critical-manufacturing-sector-cybersecurity-framework-implementation-guidance

[9] Dash, B., & Ansari, M. F. (2022). An effective cybersecurity awareness training model: First defense of an organizational security strategy. International Research Journal of Engineering and Technology (IRJET), 9(4), 1-6.

[10] Deloitte. (2016). Cyber risk in advanced manufacturing: Thriving in a world of exponential changes and opportunities. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf

[11] Fragapane, G., de Koster, R., Sgarbossa, F., & Strandhagen, J. O. (2021). Planning and control of autonomous mobile robots for intralogistics: Literature review and research agenda. European Journal of Operational Research, 294(2), 405-426 https://doi.org/10.1016/j.ejor.2021.01.019

[12] InfoSecurity Magazine (2024) IBM: Identity Compromises Surge as Top Initial Access Method for Cybercriminals. Retrieved https://www.infosecurity-magazine.com/news/ibm-identity-top-initial-access/

[13] Keshvarparast, A., Battini, D., Battaia, O., Calzavara, M., Sgarbossa, F., & Otto, B. (2023). Collaborative robots in manufacturing and assembly systems: literature review and future research agenda. *J Intell Manuf* 35, 2065–2118 (2024). https://doi.org/10.1007/s10845-023-02137-w

[14] Kusiak, A. (2017). Smart manufacturing. *International Journal of Production Research*, *56*(1–2), 508–517. https://doi.org/10.1080/00207543.2017.1351644

[15] Kumar, N., Hasan, S. S., Srivastava, K., Akhtar, R., Yadav, R. K., & Choubey, V. K. (2022). Lean manufacturing techniques and its implementation: A review. Materials Today: Proceedings, 64(3), 1188-1192 https://doi.org/10.1016/j.matpr.2022.03.481.

[16] Lee, J., Bagheri, B., & Kao, H.-A. (2018). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters, 3*, 18-23. https://doi.org/10.1016/j.mfglet.2014.12.001

[17] Meindl, B., Ayala, N. F., Mendonça, J., & Frank, A. G. (2021). The four smarts of Industry 4.0: Evolution of ten years of research and future perspectives. Technological Forecasting and Social Change, 168, 120784. https://doi.org/10.1016/j.techfore.2021.120784.

[18] National Association of Manufacturers. (2024). Manufacturing in the United States Retrieved from https://nam.org/manufacturing-in-the-united-states/#KeyFacts

[19] National Institute of Standards and Technology. (2020). Cybersecurity framework version 1.1 manufacturing profile (NISTIR 8183r1). https://doi.org/10.6028/NIST.IR.8183r1

[20] Patera, L., Garbugli, A., Bujari, A., Scotece, D., & Corradi, A. (2022). A Layered Middleware for OT/IT Convergence to Empower Industry 5.0 Applications. *Sensors*, *22*(1), 190. https://doi.org/10.3390/s22010190

[21] Rakas, S. V. B., Stojanović, M. D., & Marković-Petrović, J. D. (2020). A review of research work on network-based SCADA intrusion detection systems. IEEE Access, 8, 93083-93108. 10.1109/ACCESS.2020.2994961

[22] Rockwell Automation. (2020). Digital transformation: continuously optimizing manufacturing operations (Publication No. CE-AP001A-EN-P). Retrieved from https://literature.rockwellautomation.com/idc/groups/literature/documents/ap/ce-ap001_-en-p.pdf

[23] U.S. Government Accountability Office. (2021, May 18). Colonial Pipeline cyberattack highlights need for better federal and private-sector preparedness (infographic) https://www.gao.gov/blog/colonial-pipeline-

cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic

[24] Verizon (2023. 2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket. Retrieved from https://www.verizon.com/about/news/2023-data-breach-investigations-report