International Journal on Science and Technology (IJSAT)

E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Convergence of Information Technology (IT) and Operations Technology (OT) in Bio-Pharmaceutical Manufacturing Industry

Ravi Kiran Koppichetti

koppichettiravikiran@gmail.com

Abstract

The Industry 4.0 paradigm has redefined industrial operations by enhancing automation, machine interconnectivity, and real-time data analytics. At the core of this transformation is the convergence of Information Technology (IT) and Operational Technology (OT), bridging the gap between enterprise data management and real-time process control. While IT focuses on data governance, analytics, and cloud computing, OT monitors and controls physical assets. Their integration is essential for seamless automation, predictive insights, and optimized manufacturing workflows.

However, IT and OT operate in distinct domains with differing priorities, architectures, and security concerns, making convergence a complex challenge. This paper explores organizational and technological barriers to IT-OT integration within the biopharmaceutical manufacturing industry and presents a structured framework for convergence. This study provides a roadmap for asset-intensive industries to enhance operational efficiency, regulatory compliance, and digital transformation by addressing infrastructure interoperability, cybersecurity risks, and data harmonization.

Keywords: IT-OT Convergence, Smart Manufacturing, Industry 4.0, Digitization, Biopharmaceutical industry, Manufacturing

I. Introduction:

The fourth industrial revolution, or Industry 4.0, is reshaping manufacturing and industrial operations by integrating advanced automation, cyber-physical systems, Industrial IoT (IIoT), and AI-driven analytics. At the core of this transformation is the convergence of Information Technology (IT) and Operational Technology (OT)—two traditionally distinct domains that now require seamless integration to enhance efficiency, facilitate real-time decision-making, and drive digital transformation.

IT primarily focuses on data management, analytics, enterprise resource planning (ERP), and cloud computing, which ensures business intelligence, cybersecurity, and process optimization. In contrast, OT governs industrial control systems (ICS), programmable logic controllers (PLCs), SCADA systems, and machine automation, overseeing real-time process control and production efficiency. These two domains

have operated independently, with distinct architectures, communication protocols, and security frameworks. However, the growing demand for smart manufacturing, predictive maintenance, and real-time data analytics has made IT-OT convergence necessary[1, 2].

The transition to IT-OT integration presents both opportunities and challenges. While it enables enhanced automation, improved asset utilization, and data-driven manufacturing, it also introduces cybersecurity risks, interoperability issues, and the challenge of integrating legacy OT systems with modern IT infrastructures. The biopharmaceutical manufacturing industry, being highly regulated and asset-intensive, faces unique complexities in achieving this integration while ensuring compliance with GMP, FDA 21 CFR Part 11, and data integrity standards.

II. Information Technology

Information Technology (IT) in biopharmaceutical manufacturing involves the integration of computing systems, software, networks, and data management technologies to improve production efficiency, automation, and decision-making. Itallows manufacturers to streamline operations, enhance supply chain management, optimize production processes, and maintain quality control through advanced data analytics, cloud computing, and industrial software solutions[1, 3].

Benefits of IT in Biopharmaceutical Manufacturing

A. Enhanced Operational Efficiency

- IT-driven automation reduces manual intervention, minimizes human errors in the business, and supports tasks such as compliance and scheduling.
- Enterprise Resource Planning (ERP) and Manufacturing Execution Systems (MES) improve production scheduling and resource allocation at the corporate level and better utilize the capacity of individual manufacturing facilities.

B. Real-time Data Monitoring and Analytics

- Information Technology enables companies to collect data from IoT sensors and machinery. This data can be stored, analyzed, and visualized for predictive maintenance.
- The sensor data stored in IT databases can be analyzed to provide insights into performance trends and inefficiencies.

C. Enhanced Security and Compliance

- Information technology's cybersecurity solutions protect industrial networks from cyber threats and data breaches. These solutions ensure that Biopharmaceutical companies maintain compliance with regulatory standards.

D. Smart Decision-Making with AI and Machine Learning

- AI-driven forecasting solutions in IT enhance production planning to align with market demand. These systems utilize available data from IT databases, leveraging computing power to deliver valuable insights for the company.

III. Operational Technology

In manufacturing, Operational Technology (OT) includes the hardware and software systems that monitor, control, and automate industrial processes, machinery, and infrastructure. OT is vital for maintaining real-time control, safety, and efficiency in manufacturing environments, integrating various industrial control systems (ICS) such as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), and Programmable Logic Controllers (PLC).
Unlike information technology (IT), primarily concerned with data processing and business applications, OT is intrinsically linked to physical processes, factory floor automation, and machine-to-machine (M2M) communication. This synergy facilitates seamless industrial operations[2, 3,4].

Benefits of OT in Biopharmaceutical Manufacturing

A. Real-Time Process Control and Automation

- Operational Technology (OT) ensures precise control over manufacturing processes with minimal human intervention. The programs involved in Manufacturing Execution System (MES), Supervisory Control and Data Acquisition (SCADA), and Process Control Systems (PCS) take the requirements from humans and constantly control the equipment to produce media, active pharmaceutical ingredients (API), etc.

B. Increased Production Efficiency

- Operational Technology (OT) solutions such as SCADA and PCS systems can help companies optimize industrial workflows and reduce cycle times. These systems control robotics and automation technologies to enhance production speed and accuracy.

C. Improved Equipment Reliability and Predictive Maintenance

- Operational Technology (OT) systems allow continuous reading and storing of IoT sensor data. This data stored in the database can be analyzed using Big Data Technologies to detect machine anomalies before failures occur. This predictive maintenance reduces unplanned downtime, improving operational continuity and thus improving manufacturer efficiency and customer safety.

IV. Process for IT and OT Convergence in Biopharmaceutical Manufacturing

IT and OT convergence refers to the integration of information technology (IT) systems, which manage data processing and enterprise applications, with operational technology (OT) systems, which control industrial processes and machinery. This transformation is essential for enabling Industry 4.0, smart manufacturing techniques, predictive maintenance, and real-time decision-making [4, 5, 6].

The convergence process follows a structured approach to ensure seamless integration while addressing challenges related to cybersecurity, interoperability, data, and organizational factors.

A. Assess current IT and OT Infrastructure

- Assess the current IT and OT infrastructure by comprehensively auditing their assets, such as hardware, software, and network configurations.
- Identify the legacy IT and OT systems that may lack interoperability with modern IT and OT solutions.
- Assess security vulnerabilities in IT and OT networks.

B. Define Convergence Goals and Business Objectives

- The manufacturing company should establish clear objectives aligned with manufacturing and business priorities.
- Companies should focus on operational efficiency, reducing downtime, and optimizing production. Enabling real-time analytics and cloud-based insights can help achieve these goals [7].
- Companies should also implement a unified security framework for IT and OT systems. This framework helps them adhere to industry standards and ensure compliance.

C. Establish a Unified Network Architecture

The central IT and OT teams should integrate the IT and OT networks while ensuring security and facilitating real-time performance analytics. This integration is achievable by implementing industrial-grade networking solutions, including edge computing and secure communication protocols (e.g., MQTT, OPC UA) for IT-OT data exchange, as well as segmenting OT networks using firewalls and Virtual LANs (VLANs) to mitigate cyber threats, as illustrated in Fig. 1.

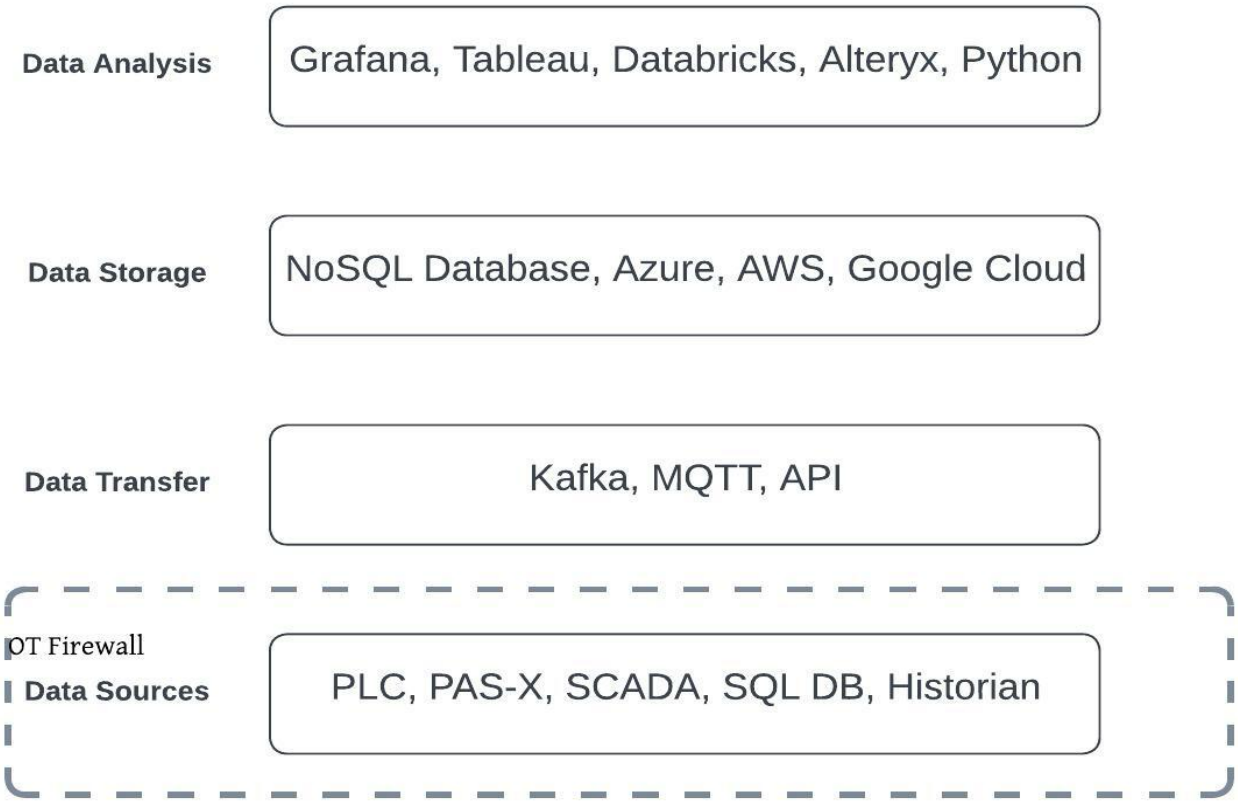

Fig. 1. Unified Data Architecture

D. Deploy Secure IT-OT Data Integration Platforms

- Manufacturing facilities should enable seamless data exchange between enterprise IT systems and industrial OT devices. This data exchange is created by connecting IoT devices or sensors with ERP and HMI layers, as shown in Fig. 2.
- Companies can utilize middleware applications or APIs to standardize the communication between IT and OT layers like PLCs, SCADA, HMI, and ERP. The data collected from OT devices can be stored in databases at the IT layer and analyzed for predictive maintenance and decision-making[8].

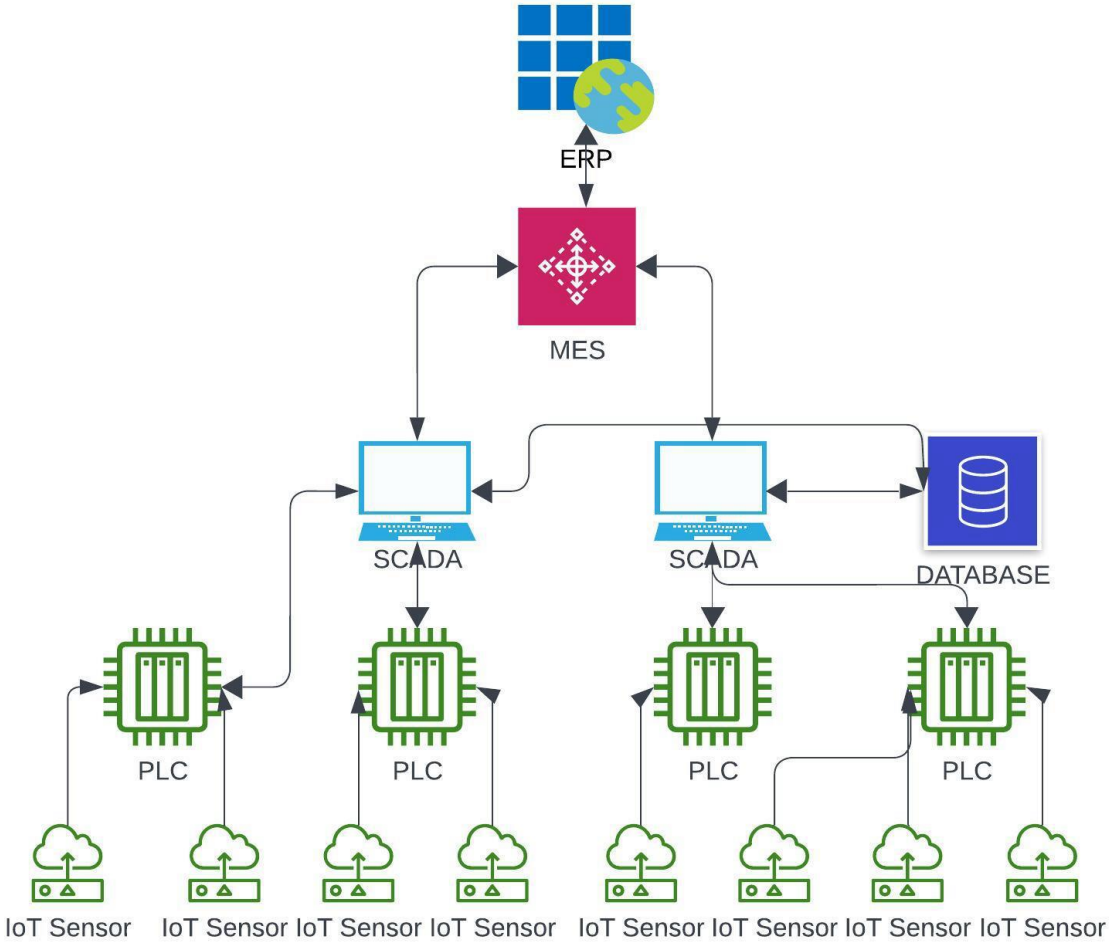

Fig. 2. IT and OT systems integration

E. Implement Cybersecurity Framework for IT-OT Environments

- Theintegrated IT and OT systems of a manufacturing facility are most prone to cyber security issues. Central IT and OT teams must protect these systems from cyber threats and unauthorized access.
- The IT security team should design and implement a zero-trust architecture for access control and ensure secure remote access through VPNs and multi-factor authentication (MFA).

F. Standardize IT and OT Governance, Policies, and Compliance

- The central compliance team should work with IT and OT technical subject matter experts (SMEs), architecture, and operations teams to develop and establish a unified governance model for IT-OT operations.
- The teams should standardize and implement industry compliance frameworks by conducting cross-functional training and bridging the skill gap between IT and OT personnel [9].

G. Pilot and Scale IT-OT Integration

- After brainstorming, designing, and developing the integration strategy, teams must validate it in a controlled environment by starting pilot projects on a single production line before fully deploying all production lines or manufacturing facilities.
- As shown in Fig. 3., Operation Technology and Information Technology processes are first integrated to find common ground on internal and external functions, creating a new business process[10,12].
- As the organization matures and moves towards servitization, such as Industry as a Service or Everything as a Service, it focuses highest on product and customer management.
- A comprehensive evaluation of real-time data processing, automation, and cybersecurity measures is necessary.

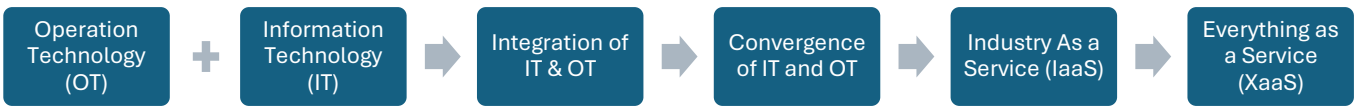

Fig. 3. Displaying stages in IT & OT Convergence

H. Continuous Monitoring and Optimization

- After converging IT and OT technologies for a single production line or entire company, teams must implement real-time performance monitoring and analytics dashboards for data-driven decision-making.
- The IT and business teams can also develop and utilize machine learning and AI capabilities to create predictive maintenance solutions and reduce downtime.
- The central IT and local OT teams should regularly assess network security, operational efficiency, and IT-OT integration success metrics.

V. Deterrents to Convergence in Biopharmaceutical Manufacturing

A. Ownership and Governance:

Currently, in most biopharmaceutical manufacturing companies, Information Technology (IT) and Operational Technology (OT) are managed by separate entities within the organization. IT is overseen and supported by corporate teams that specialize in developing and implementing company-wide IT strategies. This team is responsible for establishing standardized protocols for software and infrastructure throughout the organization.

In contrast, OT is decentralized and primarily managed by local business units or production managers. This structure often creates a lack of alignment and harmonization across different sites, as no centralized authority is dedicated to devising OT strategies. The lack of a coordinated

framework for OT further deepens the existing differences between IT and OT, making cross-functional collaboration challenging.

B. Technology Misalignment:

Traditionally, Operational Technology (OT) equipment, such as sensors, is designed to operate in tough environmental conditions, including fluctuating temperatures and pressures. In contrast, IT equipment is used and maintained in safe, clean environments.

The ongoing use of time-sharing operating systems in IT and real-time operating systems in OT, due to the absence of a standard architecture that can accommodate the needs of both IT and OT, is creating constraints. These technological misalignment constraints are hindering collaboration between teams.

C. Environmental differences:

The IT equipment of biopharmaceutical manufacturing companies is typically found in clean and well-managed environments, with systems in place to prevent failures and personnel available to address any issues that arise. Over the past 20 years, technology has advanced significantly, enabling businesses to process data more quickly and reliably. This encompasses improvements in data transfer speed, storage capacity, and the systems utilized to ensure everything operates smoothly.

Conversely, operational technology (OT) has distinct needs and functions in very different settings. OT equipment often encounters extreme conditions, such as high pressure, humidity, and temperature fluctuations. Unlike IT systems that may become outdated in just a few years, OT equipment is built to endure much longer—often between 10 to 50 years—because it must function dependably in challenging environments like factories and outdoor settings. OT devices are generally designed for specific tasks and must work with a high level of reliability, as they frequently control vital and potentially hazardous machinery. Therefore, any failures in these systems can have serious repercussions, making their reliability and integrity essential.

D. Compatibility differences:

Universal standards in computing and networking have benefited the hardware and software industry by promoting compatibility and ongoing improvements. However, achieving this compatibility is not always possible, leading companies to maintain backup systems as part of their operating costs.

Operational Technology (OT) operates in environments that require uninterrupted functionality and cannot be used in a typical business environment. Conversely, Information Technology (IT) often fails to effectively integrate with OT systems, as IT developers may not fully understand the unique safety concerns and limitations of OT.

E. Skills difference:

In most biopharmaceutical manufacturing facilities, the operational technology (OT) equipment is often older than that found in other industries, resulting in a significant difference in the skills

required to operate both types of technology. Information technology (IT) equipment is frequently updated to meet performance and safety standards, while OT prioritizes stability and compatibility with existing tools. Consequently, the skill sets required for these two areas differ greatly. IT professionals are continuously learning new software and programming languages to stay current with the latest advancements. In contrast, OT workers tend to use specific technologies for extended periods, placing a premium on reliability, which means their experience is highly valued. This often results in an older, more experienced OT workforce, whereas IT specialists are generally younger and earn less.

Moreover, OT workers typically come from traditional engineering backgrounds, such as mechanical, civil, or industrial engineering. They are trained to approach projects systematically and solve problems effectively. While IT specialists may also hold engineering degrees, they concentrate on different skills and terminology. These differences can lead to challenges in communication and planning between the two groups.

F. Security:

Operational Technology (OT) refers to the equipment used to manage and monitor physical processes, such as those in factories or power plants. This equipment is often found in secure or hard-to-reach locations, making robust physical security essential. Traditionally, these systems have been manually controlled, helping to limit their exposure to various risks.

On the other hand, Information Technology (IT), which encompasses computers and networks, has made significant advances in protecting data and systems due to ongoing cybersecurity threats, especially since the advent of the Internet [11].

However, it's not as straightforward as simply applying IT security methods to OT. Even a minor network issue in OT can inadvertently cause critical machinery to shut down, potentially leading to safety concerns. While OT can draw lessons from IT's security experiences, IT professionals must recognize the unique challenges and environments that OT systems encounter.

VI. Conclusion:

The convergence of Information Technology (IT) and Operational Technology (OT) is revolutionizing industrial operations by bridging the gap between data-driven enterprise systems and real-time process control. While IT focuses on data management, analytics, and cloud computing, OT is responsible for monitoring, controlling, and automating physical processes in manufacturing and other industrial environments. Integrating these traditionally separate domains enables enhanced automation, predictive analytics, and real-time decision-making, fostering efficiency, scalability, and regulatory compliance.

Achieving IT-OT convergence requires a structured approach that includes assessing existing infrastructure, implementing secure and standardized communication protocols, integrating IoT and edge computing, deploying AI-driven analytics, and ensuring cybersecurity compliance. Manufacturing industries, especially biopharmaceuticals, benefit from this transformation by improving productivity, minimizing downtime, and optimizing resource utilization [12].

Despite its advantages, several deterrents hinder IT-OT convergence, including legacy system incompatibility, cybersecurity vulnerabilities, high implementation costs, and resistance to change. Overcoming these challenges requires strategic investment in modern technologies, robust security frameworks, workforce training, and change management initiatives.

Ultimately, IT-OT convergence is not just a technological upgrade but a fundamental shift toward Industry 4.0, which enables intelligent, connected, and data-driven industrial ecosystems. Biopharmaceutical companies that embrace this transformation will be better positioned to drive innovation, improve operational resilience, and maintain a competitive edge in an increasingly digitalized world.

References:

[1] K. L. S. Sharma, *Information Technology–Operation Technology Convergence*, 2nd ed. *Overview of Industrial Process Automation*, pp. 359-376, 2017.

[2] T. U. Daim and Z. Faili, "Fourth Industrial Revolution," in *Industry 4.0 Value Roadmap: Integrating Technology and Market Dynamics for Strategy, Innovation, and Operations*, pp. 1-5, 2019.

[3] E. Bonnetto, B. Yannou, G. Bertoluci, V. Boly, and J. Alvarez, "A categorization of customer concerns for an OT front-end of innovation process in an IT/OT convergence context," in *International Design Conference*, May 2016.

[4] I. C. Ehie and M. A. Chilton, "Understanding the influence of IT/OT convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: An empirical investigation," *Computers in Industry*, vol. 115, p. 103166, 2020.

[5]I. Paredes, "IT/OT Convergence–Cybersecurity Beyond Technology," in *Abu Dhabi International Petroleum Exhibition and Conference*, Nov. 2020, p. D012S116R078, SPE.

[6]R. P. Kranendonk, *The convergence and integration of operational technology and information technology systems*, Delft University of Technology, 2016.

[7] R. Gharpure, A. Kardekar, and R. Vyas, "Industry 4.0 Digital Transformation: Information Technology (IT)–Operations Technology (OT) Convergence Model and its Implementation in Asset-Heavy Manufacturing Industry," *Vol. 7, No. 1*, Jan. 2022.

[8] Y. Maleh, "IT/OT convergence and cyber security," *Computer Fraud & Security*, vol. 2021, no. 12, pp. 13-16, 2021.

[9] S. Z. Kamal, S. M. Al Mubarak, B. D. Scodova, P. Naik, P. Flichy, and G. Coffin, "IT and OT convergence—Opportunities and challenges," in *SPE Intelligent Energy International Conference and Exhibition*, Sept. 2016, pp. SPE-181087.

[10]D. G. Pivoto, L. F. De Almeida, R. R. Righi, J. J. Rodrigues, A. B. Lugli, and A. M. Alberti, "Cyber-physical systems architectures for industrial Internet of Things applications in Industry 4.0: A literature review," *Journal of Manufacturing Systems*, vol. 58, pp. 176-192, 2021.

[11] T. Dhlamini and T. Mawela, "Critical success factors for information technology and operational technology convergence within the energy sector," in *International Conference on Innovations in Bio-Inspired Computing and Applications*, pp. 425-434, Dec. 2021, Cham: Springer International Publishing.

[12] R. Hayes, "Managing the successful convergence of IT and OT," Deloitte, 2020.