UNLOCKING THE FUTURE OF LIFE SCIENCES MANUFACTURING

Honeywell

EXECUTIVE SUMMARY

Life sciences manufacturers face significant disruption in a dynamic, global market. To overcome these rising complexities, they must adopt a flexible, digitally integrated operational model. Industry 4.0 — the use of intelligent digital technologies like AI-assisted predictive maintenance and near real-time quality control in manufacturing — is no longer just an opportunity, but a necessity.

In this eBook, we explore:

- How the adoption of Industry 4.0 became a necessity in life sciences manufacturing
- Common barriers to implementing Industry 4.0
- Strategic imperatives manufacturers must set across their entire ecosystem
- Case studies of successful implementations
- Why having a proven partner is imperative for success

INTRODUCTION

TRANSFORM OR BE LEFT BEHIND IN A WORLD OF DISRUPTION

A confluence of factors is reshaping the priorities — and pressures — on the life sciences manufacturing industry. From supply chain uncertainties, to surging demand for advanced therapies and intricate devices, to an unrelenting focus on speed to market, the complexities continue to mount.

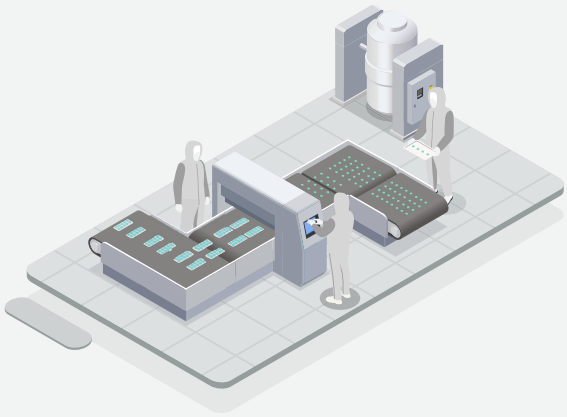
Industry 4.0 represents a transformational solution for the biggest challenges life sciences manufacturers face today. A subset of digitalization, it refers to the fourth industrial revolution, marked by the integration of cyber-physical systems, IoT, automation and real-time data in manufacturing.

Honeywell understands the potential barriers to the adoption of Industry 4.0 that exist in the life sciences industry. Barriers can be overcome through the implementation of strategic imperatives across processes, quality and compliance, the building environment, and OT cybersecurity. In doing so, manufacturers can establish key competitive advantages, while contributing to the bottom line.

A recent Deloitte report highlights one life sciences organization's projection of:

$50–75M

annual OPEX reduction after scaling digital use-cases at two pilot sites.[1]



That freed up enough capacity to avoid an estimated

$500M

in new capital expenditure for additional facilities.[1]

BARRIERS TO IMPLEMENTING INDUSTRY 4.0

Barriers can impede life sciences manufacturers from taking meaningful steps toward Industry 4.0. These include fragmented systems and manual paper trails, complicated tech transfers, growing complexities in compliance, escalating talent shortages and the rising threat of cybercrime.

The following is a detailed breakout of those five common barriers:

FRAGMENTED SYSTEMS AND MANUAL PROCESSES

There's still a heavy reliance on paper-based documentation for batch records, logbooks and standard operating procedures (SOPs) across life sciences production facilities. Each one of those thousands of manual data entries is a potential future error, compromising the accuracy and effectiveness of Manufacturing Execution Systems (MES). A biotech batch record, for example, can comprise 5,000 to 45,000 manual entries, often logged and transferred to paper. These human touchpoints can result in MES accuracy dipping to 91%, on average.[2] Solving for that 9% gap represents a significant opportunity for life sciences manufacturers to not only drive speed, efficiency and consistency, but also add to their bottom line.

COMPLICATED TECH TRANSFERS

Tech transfer — or the process of transferring a product and its associated manufacturing knowledge from one facility, team or organization to another — represents the bridge between scientific innovation and real-world patient access. Transferring a product or process from R&D to a manufacturing site often involves duplicative equipment qualification, method validation and batch testing. Poor execution can lead to costly delays, regulatory issues and lost revenue.

In addition, the rise in outsourcing the production of medical devices, drugs, biologics and other products to Contract Manufacturing Organizations (CMOs) can introduce coordination and traceability challenges. Many life sciences manufacturers don't have the infrastructure, time or resources to build these in-house capabilities. The CMOs they rely on may use different batch record formats, data platforms and SOPs that can complicate quality audits, regulatory reporting and more.

COMPLIANCE COMPLEXITY AND RISK AVERSION

In life sciences, regulatory concerns can hamper and enable innovation. In the United Kingdom, more than 80% of drugmakers reported that the Medicines & Healthcare Products Regulatory Agency's capacity and lack of predictability are legitimate barriers to drug development and manufacturing investment.[3] Similarly, more than 65% of smaller biotech firms in the United States are exploring early-stage trials outside the country due to regulatory unpredictability at the U.S. Food and Drug Administration.[4]

Validation and qualification procedures span process, equipment, cleaning and computerized systems. These can be time-consuming and involve extensive testing, documentation and skilled staffing. It's also anything but a one-time effort. Rules and regulations continue to evolve, often faster than organizations can. It can put a significant strain on organizational resources.

TALENT SHORTAGES AND TRAINING GAPS

The lack of a skilled workforce to manage modern systems, let alone optimize them, is an intensifying pain point. In the United Kingdom, life sciences manufacturers are wrestling with how to replace 75,000 retiring workers between now and 2035.[5] The U.S. Bureau of Labor reports that nearly 21% of the life sciences manufacturing workforce in the United States is age 55 or older,[6] indicating this may be a global issue.

This potential wave of mass retirement — combined with the reality that life sciences manufacturing requires specialized expertise in processing, quality control, chemistry, analytics and facility management — has companies searching for transformational solutions. Life sciences manufacturers know they need digital tools to compensate for human gaps, but they're worried about compromising quality.

RISING CYBER THREATS

While life sciences manufacturers have long prioritized the protection of IT systems, many may not provide the same level of protection to critical Operational Technology (OT) systems. With the evolution of — and dependence on — technology to drive business forward, there are now more entry points than ever before. A recent survey shows 98% of pharma companies have experienced at least one intrusion or breach attempt in the past year – nearly 50% of those experienced multiple attacks.[7]

OT and IT systems are fundamentally different and the tools designed to protect them are not interchangeable. Therefore, when organizations rely on metrics generated by IT security tools to demonstrate their commitment to OT security, they may develop a false sense of security. With the average cost of a breach in critical infrastructure rising to $4.5 million,[8] the consequences can be significant.

STRATEGIC IMPERATIVES & CASE STUDIES

To overcome those barriers, many life sciences manufacturers look to set strategic imperatives across their ecosystems — from processes, quality and compliance, building management and OT cybersecurity.

The following outlines specific imperatives in each of those key areas, along with case studies to highlight the success stories of organizations around the world:

MANUFACTURING PROCESS: FROM PAPER TRAILS TO DIGITAL WORKFLOWS

Speed and accuracy are critical drivers of success in the competitive life sciences manufacturing landscape, yet manual paper trails still inevitably slow many systems. Enter Manufacturing Execution Systems (MES), which serve as a digital nerve center to help organizations monitor, manage and control production activities — in near real time. Smart MES platforms automate batch records, recipe management, inventory and production tracking. This helps reduce human error and elevates compliance via enforcement of complex procedural controls.

CASE STUDY : SGS DRIVES GLOBAL TRANSFORMATION WITH TRACKWISE

SGS Life Sciences, a global leader in testing and certification, worked with Honeywell to address inefficiencies, limited visibility and audit complexities caused by a disconnected trail of paper-based quality processes. We guided SGS through the implementation of TrackWise Digital, a cloud-first, out-of-the-box quality management system (QMS), designed to streamline document, quality and transportation controls. Our QuickStart approach facilitated a successful rollout to 11 facilities across seven countries within the first year. The solution helped eliminate more than 25,000 paper forms and SOPs, improved audit readiness and traceability, and enabled remote operations and near-real-time reporting.

QUALITY & COMPLIANCE: STANDARDIZED, SCALABLE AND SMART

Streamlining quality and compliance activities — like corrective and preventive actions, supplier management and training — into a single, integrated QMS can help drive efficiency and consistency for an organization. Quality data can be collected, analyzed and used to make near-real-time adjustments to a process or product. The nearly seamless flow of data and unification across operations helps eliminate friction, accelerate time-to-release and enable proactive risk management.

Using machine learning capabilities for quality prediction, equipment maintenance and intelligent batch review can help reduce critical downtime by up to 15%, significantly improving equipment effectiveness.[9] Further, using near-real-time virtual models of physical assets and processes can help align demand with workforce and equipment capacity, as well as the availability of raw materials.

CASE STUDY: PHARMAMAR STREAMLINES OPERATIONS WITH CENTRALIZED PLATFORM

PharmaMar, a global leader in the discovery, development and commercialization of marine-derived oncology treatments, sought to minimize inefficiencies, data loss and compliance risks. Honeywell recommended and oversaw the implementation of a centralized digital QMS. The company achieved 100% on-time Chemistry, Manufacturing and Controls (CMC) case completion and improved data accuracy, traceability and quality insights.

THE BUILDING ENVIRONMENT: INTELLIGENT, INTEGRATED INFRASTRUCTURE

Integrating multiple building domains including building management systems, fire and life safety, security and third-party systems and equipment in an open, IoT platform can help life sciences manufacturers gain both holistic data and better control to help improve situational decision making. This can also enable building teams to better manage asset performance, access to controlled areas and indoor air quality to meet manufacturing specifications. By providing map-based control and integration with video systems, building managers can see what is happening in a building and trigger automatic workflows and procedures based on a specific situation – helping to improve response times and eliminate potential human error. Adding advanced software solutions can further enable asset reliability, predictive maintenance and energy management capabilities to provide even greater connectivity, insights and control of building performance.

CASE STUDY : LEADING CANCER CENTER OPTIMIZES FACILITY, ENERGY PERFORMANCE

Victorian Comprehensive Cancer Centre, a state-of-the-art cancer treatment and research facility in Australia, worked with Honeywell to deploy a large-scale smart campus integration project to enhance performance, patient care, compliance and more. We implemented Enterprise Buildings Integrator (EBI), a building management control system, encompassing more than 85,000 system points and 22,000 alarm-generating devices across the 1.4 million-square-foot complex. Features include Ascom messaging, Nurse Call, IPTV, queuing and wayfinding systems — all controlled by EBI and managed by our on-site Total Asset Management Team. The integration was executed with minimal clinical disruptions, while driving energy management and operational responsiveness.

OT CYBERSECURITY: SECURE BY DESIGN

Few things can hamper operations quicker than a cybersecurity with breach. They can impact processes, building operations, data, compliance, uptime and safety — and nearly 75% of OT environments experienced at least one intrusion in 2024.[10] It's critical for life sciences manufacturers to have a comprehensive and customizable OT cybersecurity solution in place. This provides continuous monitoring across manufacturing processes, MES/QMS systems and building assets. The immense value of life sciences manufacturing makes the industry attractive targets for sophisticated threat actors. Around-the-clock protections across production and building systems help deliver improved visibility, asset management, traffic analysis and near real-time threat detection.

CASE STUDY: OT CYBERSECURITY SAVES THE DAY FOR U.S. MANUFACTURER

A large U.S. manufacturing facility was the target of a potentially serious OT cyberattack when an unauthorized asset connected to its network. While the organization's traditional IT technologies failed to catch the issue, Honeywell Cyber Insights detected the rogue device and alerted the customer to act. With the OT-specific cybersecurity tools in place, the organization successfully defended against operational disruption.

THE DIGITAL FACTORY OF THE FUTURE STARTS NOW

These foundational Industry 4.0 technologies — spanning manufacturing, quality, facility operations and OT cybersecurity — work together to help life sciences manufacturers:

Operate with greater efficiency, consistency and compliance

Reduce downtime, mitigate risk and respond proactively to issues

Break down silos to data across departments and disciplines

Just as importantly, they enable scalability across modalities and sites, supporting the full range of manufacturing needs from small molecules to advanced therapies like biologics and complex equipment. With standardized systems and templates, organizations can accelerate tech transfer, simplify upgrades and reduce training requirements across global operations.

A unified digital ecosystem can help life sciences manufacturers deliver value quickly with minimal disruption, whether deploying in new environments or modernizing existing sites. This empowers them to grow smarter, scale faster and adapt to new challenges.

PARTNERSHIP IS IMPERATIVE FOR SUCCESS

Navigating the integration of Industry 4.0 calls for a proven partner who knows the unique demands and potential pitfalls of life sciences manufacturing. That partner should understand that digital transformation is a journey, not a destination — and be equipped to guide you through the following critical transformations:

- ☑ Accelerate tech transfer readiness: Standardize systems, digitize records and streamline validation to speed up new product introduction.
- ☑ Invest in scalable, modular digital platforms: Avoid vendor lock-in by adopting systems that evolve as operations grow.
- ☑ Treat data as a strategic asset: Integrate manufacturing, quality and facilities data for better insight and compliance — then use the data strategically.
- ☑ Redefine compliance as a competitive advantage: Use digital tools to reduce audit prep time, improve traceability and enable agile change.
- ☑ Build OT cybersecurity into the DNA of your operations: Use solutions built with cybersecurity and privacy in mind and design secure systems to help mitigate both reputational and financial risk.

With more than 30 years in the life sciences industry, Honeywell has experience guiding partners through all the above. We offer the end-to-end coverage of systems, people and infrastructure needed to accelerate success from the manufacturing floor to the cloud.

Why Joining Forces with Honeywell Makes Sense

30+ YEARS
of providing solutions in life sciences

3,400+
projects around the world

$9.5B
in energy and operational cost savings[11]

7,000+
cyber projects in 130+ countries

Contact us to learn how Honeywell's experience can create competitive advantages for you via digital transformation in life sciences manufacturing.

REFERENCES

1. Deloitte, "2022 Global Life Sciences Outlook," 2022 [Accessed June 20, 2025]
2. McKinsey & Company, "Operations can launch the next blockbuster in pharma," Ulf Schrader, Feb. 16, 2021 [Accessed June 17, 2025]
3. Financial Times, "UK medicines regulator needs more resources, drugmakers say," Hannah Kuchler, Dec. 3, 2024 [Accessed June 17, 2025]
4. Reuters, "Upheaval at FDA pushes some biotech firms to move early trials out of US," Maggie Fick, May 14, 2025 [Accessed June 16, 2025]
5. U.K. Bioindustry Association, "Life Sciences Will Need 70,000 New Jobs By 2035," March 5, 2025 [Accessed June 20, 2025]
6. U.S. Bureau of Labor Statistics, "Labor Force Statistics from the Current Population Survey," Jan. 29, 2025 [Accessed June 18, 2025]
7. Fortinet, "The 2021 State of Pharmaceuticals and Cybersecurity Report Rising Cyber Threats," Aug. 30, 2021 [Accessed June 17, 2025]
8. IBM, "Cost of a Data Breach Report 2024," 2024 [Accessed June 16, 2025]
9. Deloitte, "Predictive Maintenance," 2022 [Accessed June 25, 2025]
10. KPMG, "The (CS)2AI-KPMG Control System Cybersecurity Annual Report," 2024 [Accessed June 18, 2025]
11. Honeywell, "ESPC Energy and Operational Cost Saving Guarantees and Projects," Updated March 2023

For more information

https://www.honeywell.com/us/en/industries/life-sciences#contactus

Honeywell

855 S Mint St, Charlotte, NC
28202-1517 USA
www.honeywell.com

EBK-25-01-EN | 07/25

THE FUTURE IS WHAT WE MAKE IT

Honeywell