implementing pharma 4.0
overcoming obstacles to achieve manufacturing excellence
embracing security-first design

successful integrating legacy M2M/OT equipment

data-driven decision-making

future-proofing for agility and cost effectiveness

contact us
introduction

The pharmaceutical industry is undergoing rapid change: **pricing pressures, regulatory developments, and evolving technology** are forcing companies to reassess their manufacturing lines to meet new demands.

To this end, pharma companies are undertaking a digital transformation. This movement, dubbed ‘**pharma 4.0,**’ is aimed at leveraging connectivity to gain better insight and control over their manufacturing processes.

Partly due to regulatory constraints, the pharma industry is late to this ‘4.0’ movement. While the greater manufacturing industry is well on their way to adopting IoT (Internet of Things)-based capabilities, **over 50% of pharmaceutical manufacturers assess their IoT maturity as either ‘not started’ or in the ‘early stages of planning.’**

Transforming an organization from that stage can be a daunting challenge. In fact, according to a report from Cisco, **nearly 75% of IoT projects fail**. At Eurotech, we’ve spent the last 30 years innovating in the IoT space. Our engineers have helped countless companies take projects from stalled to successful. In this white paper, we’ll go through the most common pitfalls and how to prevent them.
Pharma 4.0 is the pharmaceutical industry's version of Industry 4.0, so called because it represents the digitalization of manufacturing processes likened to the fourth industrial revolution.

This 4.0 revolution is based on advancements in connectivity and computing, enabling manufacturers to:

- **Visualize, analyze, and even modify** any aspect of their manufacturing process to drive better efficiency and quality.
- **Provide transparency** from the manufacturing facility to the patient, providing greater visibility into the supply chain and automated insights into product quality.

In turn, these advancements are driving changes like:

- **Create a digital twin** of a device's software and settings to easily test upgrades before implementing them. Automate manual processes and even apply AI to reduce repetitive work and improve manufacturing consistency.

**Continuous manufacturing (CM)** – Historically, pharmaceuticals have been made in discrete steps with product often being stored and even shipped to other facilities before the next step in the development process. To an extent, this approach allowed specialization that increased efficiency. But it also
created unnecessary bottlenecks and introduced quality risks. With the dawn of stronger IoT and operational technologies, continuous manufacturing can reduce the time it takes to develop medicines up to 90% and provide a cost savings of between 30-50%.

**Automation and AI Integration** – In pharmaceutical manufacturing, an estimated 50% of existing work activities could be automated, reducing costs by 20% or more. To add to this, new advancements like new product modalities and advanced analytics have created a talent gap. Automation and AI can help fill these gaps and allow manufacturing teams to catch up to their R&D counterparts.

**Quality by Design** – Per the European Medicines Agency (EMA), “Quality by design is an approach that aims to ensure the quality of medicines by employing statistical, analytical and risk-management methodology in the design, development and manufacturing of medicines.” IoT solutions provide an important key to true quality by design by giving real-time visibility into the manufacturing process. Analysis can help flag any variation that could impact product quality where automation can help reduce variation and even provide AI-assisted quality controls.

With nearly 2/3 of drug shortages being caused by quality concerns, Quality by Design stands to have a huge impact on the pharmaceutical supply chain.

**Sustainability by Design** – To reduce the environmental impact of their manufacturing activities, companies are embracing sustainability by design. This means developing products from the ground-up to reduce waste, resource utilization, and emissions. IoT solutions impact this process by providing key insights into resource utilization and environmental impacts. These insights can then be used to identify and remediate areas of excessive impact. For example, Eurotech customers have used IoT solutions to track energy consumption and develop solutions that cut their utilization by over 20%.

“an estimated 50% of existing work activities could be automated, reducing costs by 20% or more.”
The foundation of any digital transformation is ensuring continuous, thorough, and reliable data communication. Achieving this requires an IT/OT integration that can deliver a complete edge-to-enterprise view. This requires connecting equipment including industrial control systems, environmental sensors, visualization equipment, and more. With this 360-degree view of production, software tools can help you:

- **Monitor and address data** needs in the production environment
- **Centralize data** on one platform for analytics and machine learning

The first step to IT/OT integration is to take stock of your current digital maturity and plan steps for a more holistic integration:

- **Develop tools** to alert for inconsistencies and identify improvements
- **Inform and implement automation** and process enhancements

- Understand what aspects of your production are already computerized
- Assess how data flows during production and where you need additional connectivity
Consider the **quality of the data** you’re receiving –

- Do you have real-time visibility or does that need to be established?
- How accurate and transparent are your records?
- What is still paper based/pre-digital?

Then, **prioritize your integrations** by focusing on your end goal:

- What are you trying to improve first?
- What data is required?
- What is your next priority?

Take care to future-proof your solution by creating a framework that allows you to build in additional IT/OT integrations as you move forward.

With a use case in hand, you can begin planning your first phase of digital transformation.
conquering hurdles to ensure success

In our experience, there are 3 hurdles that determine the success or failure of IoT projects:

1. **embracing security-first design**
2. **successfully integrating legacy M2M/OT equipment**
3. **future-proofing for agility and cost effectiveness**
emerging security-first design

Arguably the most common cause of unsuccessful IoT projects is the failure to plan for security from the initial stages of project development.

Securing IoT devices is not a simple task. A single security product solution cannot enable end-to-end security; there is no silver bullet; it is essential to look at the entire system.

“Security must be a fundamental part of the overall architecture of an IoT project, i.e., be built in, not added afterwards,” explains Don Steed, director of solutions architecture at Eurotech. “Because of this, trying to retroactively add security measures into a completed project is incredibly complex and can easily stall an otherwise successful IoT project.”

When approached properly, security measures are taken at every step from the device through the cloud. These measures, called ‘hardening,’ safeguard the connectivity system against any external influence.

“Eurotech’s IoT solutions are designed to meet security standards like IEC 62443 and PSA” and integrate advanced security features like “managed X.509 certificates for authentication and secure communication in addition to software lifecycle management, secure boot, standards-based device attestation (in a partnership with GlobalSign), and support for hardware root of trust (TPM 2.0) for robust device security.”

Quadrant Knowledge Solutions, SPARK Matrix: Industrial IoT (IIoT) Platforms 2021
Physical hardening means physically changing the device or firmware to prevent tampering. This includes things like disabling unnecessary ports and creating a ‘secure boot’ that ensures the device uses only trusted software.

The software sitting on the edge requires its own hardening. This includes creating a ‘chain of trust’ between the software on the device and any cloud or on-premises server it may be communicating with. This ensures communication only occurs between the appropriate parties, making it challenging for a ‘bad actor’ to enter that chain of communication.

Still, the more times an IoT device is communicating with a ‘cloud’ or server, the more opportunities for ‘bad actors’ to get into the system. So, in addition to creating a ‘chain of trust,’ many companies will use some level of ‘edge computing’ to select a subset of data for communication on the device, rather than communicating all raw information. This limits access points into the system and ensures the program is robustly secure while maintaining program efficacy.

At Eurotech, our edge development software (part of our Everyware Software Framework, or ESF) allows developers to build their solution with a holistic approach to security – from physical device hardening to robust edge software and a secure cloud connection. By design, the platform simplifies the process of developing both their solution and robust security plan: many customers have a POC up and running in a matter of days with a final product ready in weeks.
Most IoT edge solutions are based on the integration of sensors, actuators, PLCs, field buses and protocols. Quite often, the specific combination of new and legacy OT technology is the first challenge to overcome when creating an IoT solution. For example, PLCs are normally connected through serial or LAN interfaces using field-bus communications protocols. While some of these technologies and protocols are open standards, there are literally hundreds that are proprietary and specific to vendors and vertical solutions.

These different devices, operating systems and programming languages employed on edge infrastructures represent a major barrier for companies that may not have the time and resources to untangle this communication web.

This communication web creates another challenge: security. The sheer inconsistency in standards has created a very vulnerable IoT ecosystem. Vendors use different hardware, software, and third-party services, as well as APIs and patch methods. By contrast, a truly secure IoT infrastructure would establish standard methods for device discovery with secure identify, authentication, and encrypted communications. Without this standardization, the underlying protocols are subject to abuse.

There are two ways to solve this challenge. The simplest, yet most expensive solution is to

---

2 successfully integrating legacy M2M/OT equipment

---
replace the old equipment with new, IoT-ready devices. This new equipment would integrate an IoT gateway that can send the appropriate data directly to the cloud in a standardized, secure manner. This so-called “greenfield” solution is ideal for newborn companies. For most organizations, however, completely replacing old equipment is simply not feasible. Instead, there is the need to adapt current equipment to the IoT project requirements. In this case, field assets must be retrofit with sensors or IoT smart devices and gateways. Since the industry lacks standardized, open protocols, M2M machinery and components (such as sensors, actuators, and PLCs) will often communicate with different protocols, leaving the organization to try and integrate a crowd of devices with different protocols into their IT/cloud application.

This, in turn, adds to the project workload and creates security challenges that must be addressed. So, what is the solution? **Work with a partner that can integrate edge hardware and software solutions that enable a mixture of protocols and data transformation.** Their solution should be secure, completely managed, integrated, and based on open standards. In this way, they will solve all the above-mentioned issues while giving you flexibility to securely expand your solution over time.
future-proofing for agility and cost effectiveness

Future proofing an IoT solution can help ensure it will remain relevant and effective as technology and business needs evolve. To future-proof your offering, you will want to consider:

1. **Design for scalability:** Consider how the project will scale as the business grows and the number of connected devices increases.

   - In your current planned design, where are your limiting factors? Can you design the architecture modularly so the system can be easily expanded and upgraded to avoid these challenges?

2. **Consider partners that design for scalability.**

   **Understand if they:**

   - Leverage open-source protocols that give the user greater flexibility to meet current and future needs
   - Create a modular design that allow users to choose only the components necessary
for their solution - reducing the size and complexity of the OS (Operating System) while optimizing functionality.

Use the same distribution across a variety of devices through built-in compatibility.

3. Prioritize Agnosticism: Choosing agnostic partners will allow you to remain agile as your digital maturity progresses. As you look to add IoT-based capabilities, you will likely need to pull in additional technology platforms or solutions. This is where vendor lock-in can limit your growth potential. By comparison, if you are working with agnostic partners, you can have your choice of future upgrades and changes.

Design with Security First: As discussed, security is a critical consideration for IoT solutions. Regulations are constantly changing to meet the growing industry’s needs, so meeting security best practices from the outset can help ensure you have created a solution that will remain relevant. Consider building this security plan into your product as early as your first proof of concept. By having a security-first mindset, you can avoid technical challenges when it comes time to scale.

At Eurotech, we operate in some of the most demanding cybersecurity environments. Our solutions are based on open-sourced protocols wrapped in best-in-class security layers. This approach allows us to capitalize on the thought-leading open-source community while providing the vetted security of an established IoT leader.
conclusion

Pharma 4.0 will be a true revolution in pharmaceutical manufacturing. Companies that can implement IT/OT integration will be able to more seamlessly capitalize on the advancements in automation, process optimization, and quality assurance.

While the challenges associated with IT/OT integration are significant, the path is well paved. Partners like Eurotech can help provide the building blocks that allow for a successful, sustainable IoT solution.

Are you looking to start a new IoT project?

Would you like help overcoming IT/OT integration challenges?

We’re here to help!

Contact our experts today.
sources


eurotech.com