# Bridging IT and OT:

## Challenges and Opportunities

Macrium Software
It's our business to protect your data

www.macrium.com

# Bridging IT and OT: Challenges and Opportunities

Unlocking the potential of Operational Technology (OT) data is a game-changer for manufacturing organizations across multiple industries. Delving into this treasure trove enables manufacturers to craft superior products by diving into real-world usage, predicting maintenance requirements, and tailoring solutions to meet customer demands easily. By analyzing OT data, manufacturers can make informed decisions, driving continuous improvement and innovation. Ultimately, OT data empowers manufacturing organizations to optimize operations, improve customer satisfaction, and stay competitive in evolving markets.

However, unlocking the potential of OT data isn't easy. There is a fear that exposing OT devices and equipment within ICS and SCADA environments opens a vector of attack that is particularly vulnerable. OT environments are often part of critical systems where any attack or unforeseen downtime could have a massive impact.

In this comprehensive guide, we explore the critical importance of OT data, its intersection with Information Technology (IT), and the multifaceted challenges and opportunities inherent in OT management.

# CONVERGENCE OF IT AND OT

When we think about IT equipment, typically it comprises off-the-shelf devices, which are easily replaceable, and with a lifespan averaging 3 to 5 years. Maintenance is often straightforward, and they commonly operate on widely-used operating systems such as Windows, iOS, and Linux.

On the other hand, OT devices are purpose-built, featuring specialized software and often proprietary protocols. Their average lifespan is significantly longer, designed to withstand the operational demands of industrial settings that span years, if not decades. Given their critical role in managing essential infrastructure, these devices may need to run continuously without interruption.


As a result, OT systems are not as frequently updated as their IT counterparts and may harbor a number of software vulnerabilities. For example, in 2023, at least **68 cyber attacks caused physical consequences to operational technology** networks across more than 500 sites. Some of these attacks caused up to $100 million in damages.

Although modern OT devices offer remote connectivity and device management, they may not necessarily get connected because of network limitations. There are a lot of legacy OT devices for example, that are not connected. Accessibility can also pose challenges, especially when devices are situated in remote or harsh environments. For example, in the Oil and Gas industry, OT devices such as sensors and control systems are often deployed in offshore drilling rigs or remote fields, making troubleshooting and maintenance difficult.

For some organizations, control over OT devices might extend to external partners or vendors, complicating modification processes. Any alterations, including simple software updates, may require thorough approval due to the potential ripple effects on industrial processes. Here's a breakdown of the overlap between these two domains:

## Data Integration

IT and OT systems traditionally operated in silos, with IT managing enterprise-level data and OT overseeing operational processes and control systems. However, as businesses seek to optimize efficiency and gain actionable insights, there's a growing need to integrate data from both domains. This integration allows for a comprehensive view of operations, enabling better decision-making and resource allocation.

## Interconnected Systems

With the rise of IoT (Internet of Things) devices and smart sensors in industrial environments, the lines between traditional IT networks and OT networks are blurring. These interconnected systems generate vast amounts of data that can be leveraged to monitor equipment performance, predict maintenance needs, and improve overall operational efficiency.

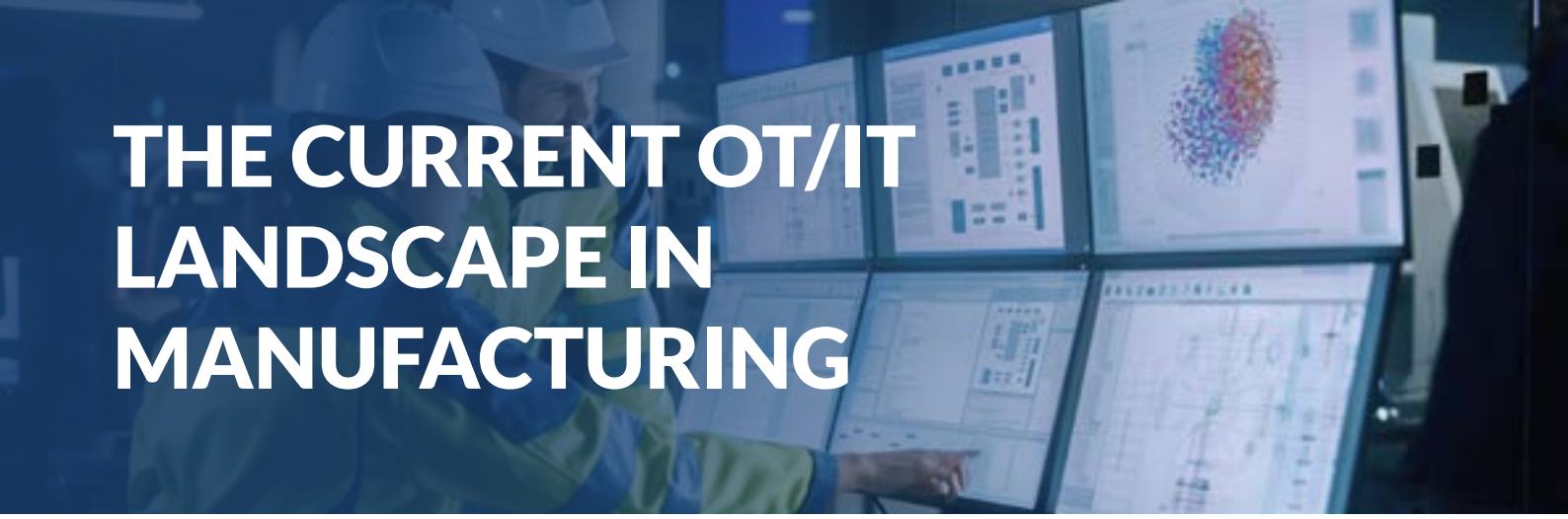
## Cybersecurity Concerns

The convergence of IT and OT data brings about new cybersecurity challenges and vulnerabilities. While IT systems have robust security measures in place to protect against external threats, security in OT environments is traditionally achieved with air gapped networks. As a result, the integration of IT and OT data requires careful consideration of cybersecurity protocols to safeguard critical infrastructure and assets from cyber attacks.

## Analytics and Insights

By combining IT and OT data, organizations can unlock valuable insights that drive innovation and business growth. Advanced analytics techniques, such as machine learning and predictive analytics, enable the identification of patterns, anomalies, and optimization opportunities across the entire operation. These insights empower organizations to make data-driven decisions that enhance productivity, reduce downtime, and increase competitiveness.

As IT and OT environments become more interconnected, organizations must handle the challenge of managing and securing their shared data to unlock its full potential and minimize risks. More complex backup strategies are required to balance what really needs backing up, including systems rather than just data. It's important that more efficient backup strategies are used, for example, those that don't saturate the network or absorb computers during operating hours.



# THE CURRENT OT/IT LANDSCAPE IN MANUFACTURING

In today's digital landscape, the convergence of IT and OT data is reshaping industries and redefining the way organizations operate. Traditionally siloed, IT and OT systems are now intertwined, driven by the need for greater efficiency, automation, and connectivity. This convergence brings together the worlds of enterprise IT infrastructure and industrial control systems, unlocking new opportunities for data-driven insights and operational optimization.

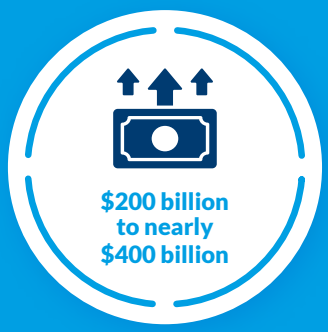
70% of manufacturing companies have already started their IT/OT convergence journey. This indicates that IT/OT convergence is no longer just a future trend, but a current reality for the majority of manufacturers. 29% of manufacturers reported having integrated their IT and OT systems, suggesting that about a third of manufacturers have successfully bridged the gap between their OT and IT systems. This has enabled them to leverage OT data more effectively for decision-making and operational improvements. However, the majority are still in the early stages of this journey.

Although manufacturers are increasingly recognizing the value of OT data, many are still struggling to harness its full potential. A significant portion of OT data remains underutilized.

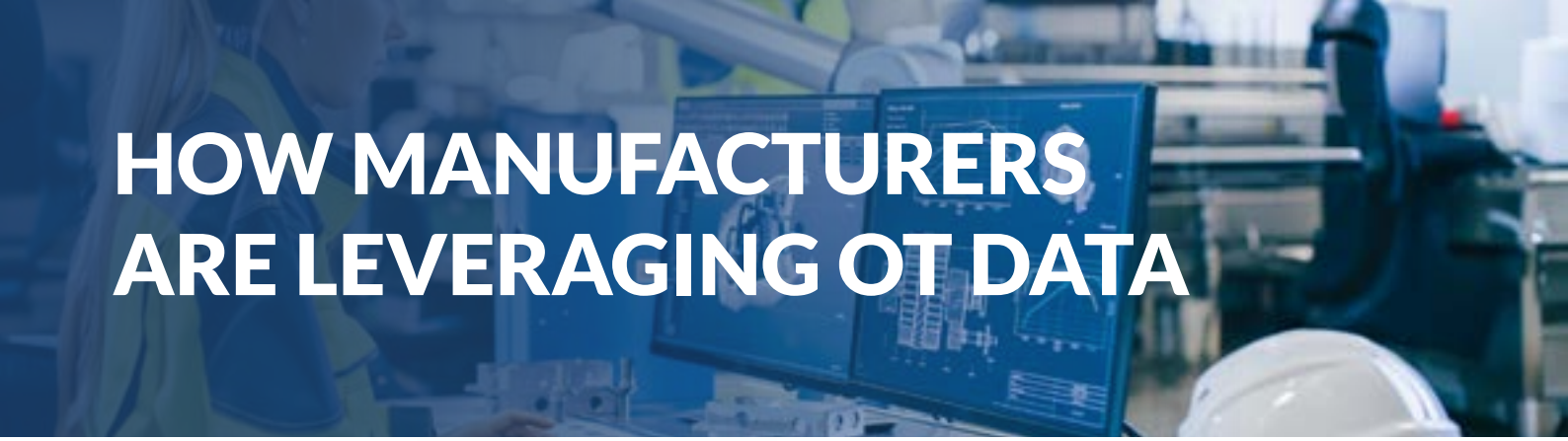

In fact, **80% of manufacturing data** generated in the last two years has not been fully leveraged, highlighting a substantial gap between data creation and data utilization. This underutilization of OT data is a missed opportunity for manufacturers to drive efficiency and innovation.

One of the major challenges in the IT/OT convergence process is transparency. Nearly 44% of companies report difficulties in achieving transparency in performance metrics related to IT/OT convergence. This lack of clarity can hinder the ability to make informed decisions based on OT data. Additionally, 37% of manufacturers highlight a lack of process control in production, which is a key area where IT/OT integration can provide significant benefits. By addressing these transparency and control issues, manufacturers can improve their operational efficiency and product quality.

Security remains a critical concern in the OT landscape. A security study revealed that manufacturing is the sector with the highest percentage of affected OT devices still in use, accounting for 26% of such devices.




This underscores the importance of implementing robust security measures to protect OT data and devices from cyber threats. As the industrial automation and software market, heavily reliant on OT data, is **projected to grow from $200 billion to nearly $400 billion** in the next six years, ensuring the security and effective utilization of OT data will be paramount for manufacturers aiming to stay competitive and innovative.



# HOW MANUFACTURERS ARE LEVERAGING OT DATA

Leveraging OT data is a powerful strategy for manufacturers looking to enhance product design, optimize performance monitoring and predictive maintenance, and ultimately improve customer satisfaction. A study by Deloitte found that organizations implementing IT/OT convergence reported 15-20% improvement in operational efficiency. This includes reduced downtimes, improved asset utilization and enhanced predictive maintenance capabilities. Let's take a look at a couple of examples below, of how manufacturers are leveraging OT data.

## Toyota

Global automotive manufacturer Toyota, utilizes OT data from its manufacturing processes to implement the principles of "lean manufacturing" and "just-in-time" production. By analyzing real-time data from sensors embedded in production equipment, Toyota can identify and eliminate waste, optimize inventory management, and ensure efficient use of resources. This approach helps Toyota maintain high levels of productivity while minimizing costs and lead times.

## GE Aerospace

Another example is GE Aerospace, the global provider of aircraft engines. GE collects OT data from aircraft engines, turbines, and other critical components using its proprietary "Digital Twin" technology. By creating digital replicas of physical assets and continuously monitoring their performance using sensor data, GE can predict maintenance needs, optimize fuel efficiency, and extend the lifespan of aircraft engines. This proactive approach to maintenance helps airlines minimize downtime, reduce operating costs, and enhance safety.

These examples highlight how leveraging OT data can drive tangible business outcomes for manufacturers, ranging from improved operational efficiency to enhanced customer satisfaction.

**Find out more about how you can safeguard your organization from disaster.**
**Take a look at how Macrium supports manufacturers with data backup and recovery.**

**LEARN MORE**

# CHALLENGES WITH OT DATA COLLECTION AND ANALYSIS

## Challenges of OT data

One of the hurdles in handling OT data lies in its sheer volume and diversity. OT systems generate copious amounts of real-time data, which can be daunting to sift through and make sense of. Moreover, this data comes from various sources like sensors, machinery, and control systems, adding complexity to integration and analysis efforts.

Ensuring the accuracy and reliability of OT data poses another significant challenge. Given the critical role of OT systems in industrial operations, even minor inaccuracies can lead to significant repercussions. Robust validation and cleansing processes are vital to maintaining data integrity and trustworthiness.

Security is also a concern when dealing with OT data. With OT systems often connected to the internet, they become potential targets for cyber threats. Protecting the confidentiality and integrity of OT data is paramount to prevent unauthorized access or tampering. The need to protect OT systems with robust backup is important. When systems inevitably go down, resilient backup and recovery processes are vital to get things up and running.

## Effects of Cyber Attacks on OT

Cyberattacks targeting OT tend to inflict more severe consequences compared to those targeting IT, as they can result in physical damages such as shutdowns, outages, leaks, and even explosions.

**In 2021, there was a notable surge in OT cyberattacks**, with 64 incidents reported publicly, marking a 140 percent increase from the previous year. Shockingly, around 35 percent of these attacks led to physical consequences, with an estimated average damage of $140 million per incident.

Cybercriminals frequently exploit vulnerabilities in OT devices using ransomware and less-secured third-party connections, causing disruptions in production and operations. Industrial and manufacturing organizations often face a number of technical and operational challenges in safeguarding against such attacks. For example:

- Legacy systems pose significant security risks due to outdated vulnerabilities and limited security measures.
- Managing security controls on legacy OT devices, supplied before cybersecurity became a focal point, presents challenges, as does grappling with third-party remote connections to control OT devices.
- The ambiguity surrounding ownership between OT and IT teams further complicates efforts to centralize, manage, and govern OT cyber operations.
- The competing priorities of OT decision-makers, torn between increasing productivity and securing devices, exacerbate the challenge. A shortage of skilled professionals with expertise in both cybersecurity and automation control systems further hampers mitigation efforts.
- Business, operational, and technical constraints also hinder the timely implementation of security solutions, with continuous processes sometimes running for years before a planned shutdown allows for updates and patches.

These challenges highlight the importance of striking a balance between business continuity i.e. "keeping the lights on", and essential strategies with IT to mitigate disaster risks. Collaborative efforts between OT and IT teams are needed to bolster OT cybersecurity and safeguard critical infrastructure.

# ADVANTAGES OF LEVERAGING OT DATA FOR MANUFACTURERS

Despite these obstacles, there are ample opportunities associated with OT data analysis. Some of those include:

## Product performance and usage

By tapping into the insights gleaned from OT data, manufacturers can gain valuable insights into product performance and usage patterns. This knowledge can fuel improvements in product design, maintenance strategies, and overall customer satisfaction.

## Predictive maintenance

Leveraging OT data enables manufacturers to detect and predict equipment failures or anomalies in real-time. Implementing predictive maintenance based on OT data analysis helps minimize downtime, cut maintenance costs, and prolong product lifespans.

## Value-added service for customers

OT data analysis empowers manufacturers to offer value-added services to customers, enhancing their competitive edge. OEMs can proactively support their customers by remotely monitoring industrial equipment and providing predictive maintenance services, minimizing disruptions, and delivering superior experiences.

## Data protection and security

With the increasing digitization of industrial processes, data protection, and security have become paramount concerns for manufacturers. By implementing robust data protection measures, such as encryption, access controls, and threat detection systems, manufacturers can safeguard sensitive OT data from unauthorized access, cyber threats, and data breaches. This ensures their data's integrity, confidentiality, and availability, enhancing trust and reliability in their products and services.

Despite the challenges, the opportunities presented by OT data far outweigh the obstacles for manufacturers. By harnessing OT data effectively, manufacturers can elevate their product offerings, streamline operations, and set themselves apart in the market.

# STRATEGIES FOR EFFECTIVE DATA UTILIZATION

Manufacturing organizations have a myriad of strategies at their disposal to effectively leverage OT data. These include, ensuring seamless data integration, promoting interoperability, implementing data security measures, and cultivating a culture driven by data insights. Let's delve deeper into each of these essential components.

## Ensure data integration

OT data often comes from diverse sources, such as sensors, machines, and control systems. It is crucial to have a robust data integration strategy in place to consolidate and analyze data from these different sources. This can involve implementing data integration platforms or leveraging APIs to connect various systems.

## Ensure data interoperability

OT data may be stored in different formats and structures, making it challenging to analyze and derive meaningful insights. Standardizing data formats and ensuring interoperability between different systems can facilitate data analysis and utilization.

## Ensure data security

OT data is valuable and sensitive, and its security should be a top priority. Manufacturers should implement robust security measures, such as encryption, access controls, data backup and recovery tools, and intrusion detection systems, to protect OT data from unauthorized access and ensure business continuity.

## Select analytics tools and technologies

Various data analytics tools and technologies are available in the market. Manufacturers should carefully evaluate their needs and select the tools that best meet their requirements. These can include machine learning algorithms, predictive analytics software, and data visualization tools.

## Foster a data-driven culture

Manufacturers should foster a data-driven culture within their organization to effectively utilize OT data. This involves promoting data literacy, providing training and resources for employees to understand and analyze data, and encouraging data-driven decision-making at all levels.

By following these strategies, manufacturers can maximize the value of OT data and effectively utilize it to drive business outcomes.