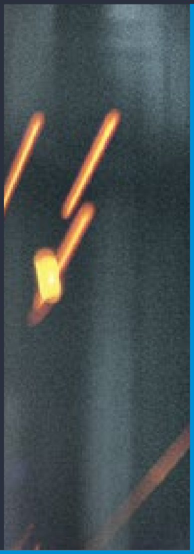
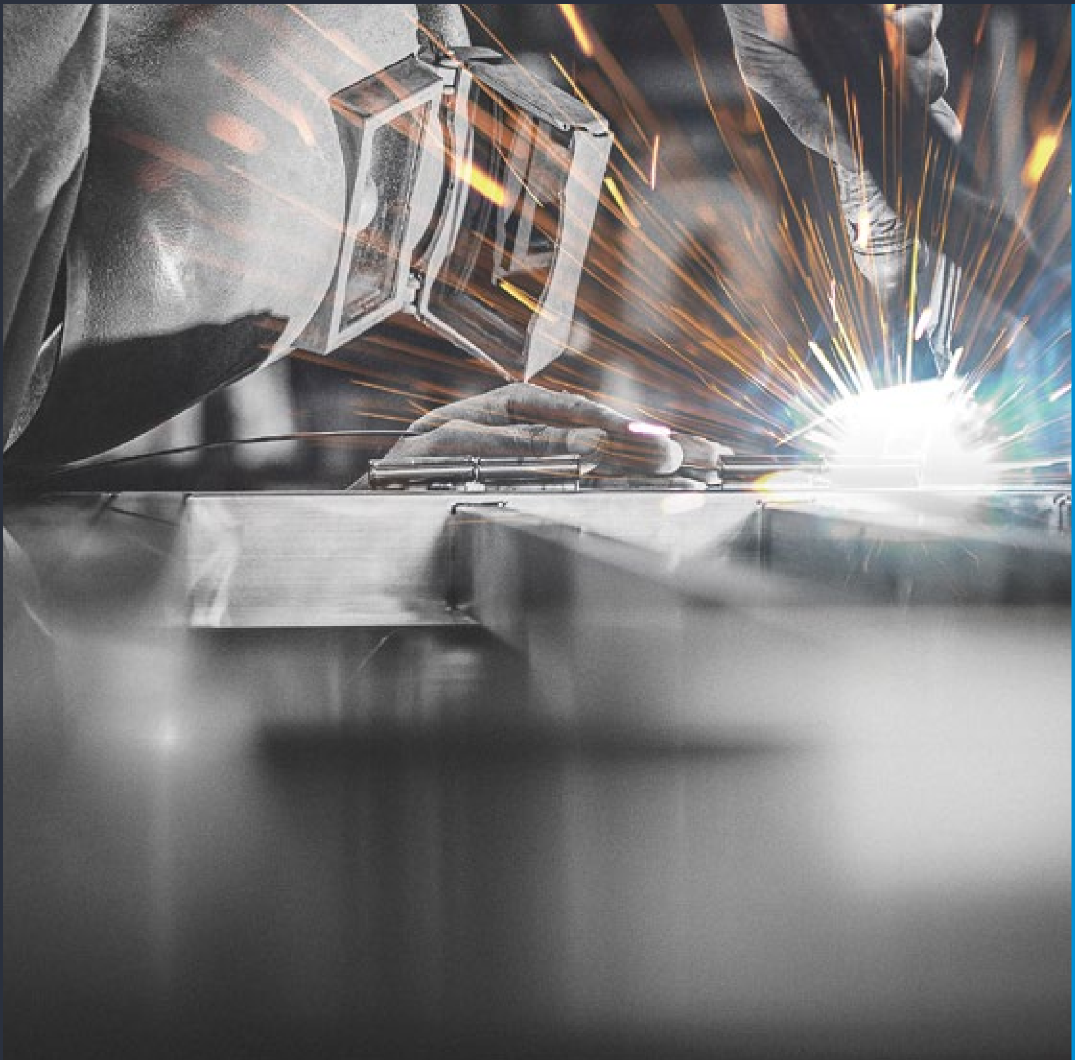
US
Center for
Advanced
Manufacturing

State of US Manufacturing





2024

US
Center for
Advanced
Manufacturing

CREDITS

Director:
Cynthia Hutchison

Editorial:
Nicole Kampe
Dennis Burck

Design:
David Tesnar
(Firehead Creative)

Support and Outreach:
Shree Parikh
Jordan Winkels
Stephanie Wright

CONTRIBUTORS

Jay Lee
Steven Dunlop
Mike Wilkes
Jim Davis
Sriram Narayanan
Alok Raj
John Carrier
Stephanie Wright

ABOUT

The US Center for Advanced Manufacturing is a non-profit organization founded in 2022 and headquartered in Troy, Michigan. We are a primary source and host for industry insights – particularly in the Fourth Industrial Revolution – and diverse voices and collaborations focused on Advanced Manufacturing in the United States. The Center is the first US entity to operate in partnership with the World Economic Forum to advance and strengthen its global manufacturing initiatives and is one of 16 World Economic Forum Centres for the Fourth Industrial Revolution.

MISSION

The US Center for Advanced Manufacturing drives state, regional and national initiatives that accelerate and strengthen advanced manufacturing in the US, while helping to inform the global manufacturing agenda. As a community, we ignite potential by harnessing the power of the people and technology through our work. We strive to build an ecosystem that accelerates change to transform manufacturing as a whole by fostering global action borne from local identity. We are an innovative voice for change in advanced manufacturing for the United States.

TABLE OF CONTENTS

Foreword

Cynthia Hutchison
CEO, US Center for
Advanced Manufacturing

What is the state of US manufacturing, and why do we need another document clarifying it?

The state of US manufacturing is more complex and dynamic than ever, and understanding it requires more than just traditional metrics like employment figures and production capacity utilization. These metrics provide only a partial view in an era of rapid technological advancements.

Relying solely on static metrics to inform policies on dynamic issues is perilous for government and manufacturers. Without accurate benchmarking and blueprints for the future, companies predominantly focused on meeting customer needs—rather than investing in R&D or pilot projects—risk creating a fragmented US supply chain. This fragmentation leaves it ill-prepared for the consequences of failing to rapidly invest in essential digital assets needed to boost productivity and resilience.

90%

of the US value chain is composed of small to midsize manufacturing enterprises

40%

of the US manufacturing workforce are employed by small manufacturers

From working in multiple corners across our nation, The US Center for Advanced Manufacturing is in a unique position to get a pulse on where we are domestically, while looking globally at the rates of Advanced Manufacturing and subsequent expanded footprints and GDP.

So, where are we and where are we going? To determine answers to these questions, we enlisted the help of top academic specialists in Industry from six US universities to collaborate on a single cohesive narrative that will inform policy makers, share learnings from those leading in the advanced manufacturing space, and provide a blueprint for the small to midsize manufacturing enterprises, which compose over 90% of the value chain.

In the State of US Manufacturing, we will share academic vision, corporate best practices, and tangible workforce initiatives and recommendations. Surveying industries throughout 2023, the US Center has received candid observations on how and when government intervention should be utilized to support accelerating digital manufacturing. While our nation's largest manufacturers are leaders in digital transformation technologies, policy intervention may be required to ensure that knowledge is disseminated downstream to small manufacturers, who employ 40% of the US manufacturing workforce.

With shared national insight, we can form an accurate representation of the state of US manufacturing, and a foundation to make critical decisions regarding industry for the future.

We extend our gratitude to all the companies and universities that contributed to this report. We are honored to present the US Center for Advanced Manufacturing's State of US Manufacturing Report for 2024 and look forward to continuing to serve you.

01

Smart Manufacturing

Stephan Biller

Harold T. Amrine Distinguished Professor,
School of Industrial Engineering & Mitchell E. Daniels, Jr. School of Business
Director, Dauch Center @The Daniels School of Business of Business
Purdue University

Steven Dunlop

Managing Director
Dauch Center @The Daniels School of Business
Purdue University

Dr. Angus I. McLeod

Global Leadership Coach
Wharton College, U. Penn, and international clients

Roy Vasher

Retired Senior Executive for IT and Supply Chain at Toyota Manufacturing NA

PURDUE UNIVERSITY®

1.1 INTRODUCTION

This report is intended to provide manufacturing SME management with a roadmap and guide to move their organization from its current state on a path to a Smart Factory. It is important to understand that this is a step-by-step process and that it will take several years for most companies to achieve a fully functional Smart Factory. Some early stage companies may decide to limit the more advanced levels of adoption.

This report will be a critical resource for manufacturers, government agencies and technology companies. It comes as the US looks at safer and more resilient manufacturing bases and supply chains.

While this chapter focuses on business processes and technology, there is an equal priority that must proceed in parallel and that is for companies to develop smart people skills for their workforce. All levels of the organization's workforce should be educated in the capabilities and operation of smart technology and leadership; supervisors must have competency on people skills such as motivation, empowerment, and coaching. There are pitfalls for those that do not embrace smart people development.

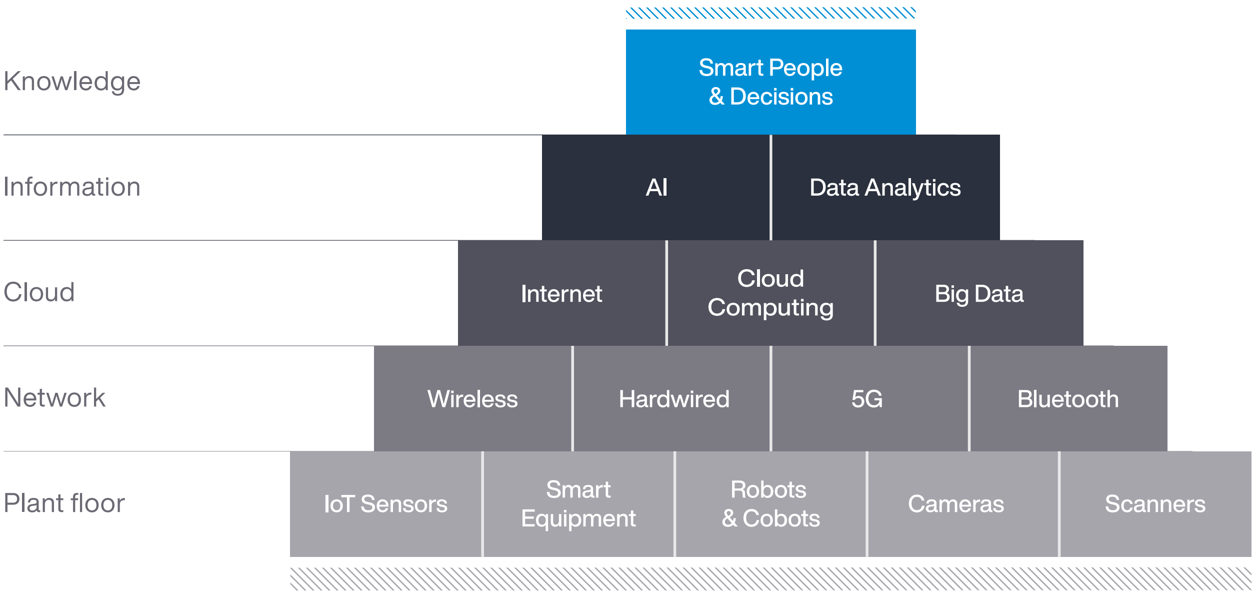
1.2 WHAT IS A SMART FACTORY?

A smart factory is a highly digitized and connected production facility that relies on smart manufacturing. The smart factory requires an internal factory-wide computer and communications network to be implemented to connect (IoT) devices. The Internet of Things (IoT) is the network of physical objects, devices, vehicles, buildings, and other items embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data.

There are several terms that are synonymous with smart factory, such as: Industry 4.0, smart manufacturing, advanced manufacturing, and digital transformation to name a few.

The figure below shows the multiple layers that are required to form the "Smart Factory Pyramid". The primary goal of implementing a comprehensive smart factory solution is to enable management and plant floor workers to make "Smart Decisions" faster. The components of this pyramid, starting at the bottom or foundation, are:

SMART FACTORY DECISION PYRAMID



Knowledge: Smart People & Decisions

Information: AI, Data Analytics

Cloud: Internet, Cloud Computing, Big Data

Network: Wireless, Hardwired, 5G, Bluetooth

Plant floor: IoT Sensors, Smart Equipment, Robots & Cobots, Cameras, Scanners

Figure 1 - Source: Purdue Dauch Center

Plant Floor Layer

This is where the products are produced and where most of the workers perform their duties. Some of the equipment such as scanners and cobots are visible and interact with the workers. However, other items such as cameras and IoT sensors attached to legacy equipment are less visible and operate autonomously.

Network Layer

Connectivity is a key component to enable raw data from the plant floor and supply chain to get uploaded in real-time to the cloud. This is accomplished in most cases by multiple means. In a plant that has a high level of noise interference it may be necessary to hardwire equipment to the network; however, some equipment may be connected via Blue Tooth, wireless, or 5G (Cellular).

Cloud Layer

The Cloud is located on the internet where software applications reside and where Big Data is stored. There are two types of applications: Transactional applications such as ERP generated process transactions to support business operations; Data Warehouse software records of raw data including video, audio, as well as data in Big Data Warehouses for both analysis and for historical archiving.

Information layer

Data stored in these large Data Warehouses are analyzed in real-time by Artificial Intelligence (AI) and Data Analytics tools (such as Power BI), to create dashboards and alerts that are presented to knowledge workers and management.

Knowledge layer

Armed with the right data at the right time, knowledge workers and management can make smart decisions faster. For example, a maintenance team gets an alert that a critical machine is predicted to break down; another, where management learns that the production rate has dropped significantly in the last hour. In both cases, the appropriate individual can investigate the issue before it causes major impact.

1.3 WHY IS A SMART FACTORY NECESSARY?

US manufacturing is in a major disruption period that makes it extremely challenging for manufacturing executives to make the necessary changes to keep pace. This is especially true for many SMEs that do not have the resources to plan for their future, because they are less cash-rich and/or more focused on day-to-day operations.

What are the key challenges during this disruptive period?

- Digital transformation
- EV transition
- Supply chain disruption
- Workforce shortage and work ethic.

Although there are many others that impact individual companies, these are the factors that have an almost universal impact across not only the manufacturing sector, but also most businesses.

Digital Transformation

Many SMEs are not equipped to create a strategic roadmap to digital transformation or smart factory. Therefore, they are at risk of falling behind their competitors. A Rockwell report states that there is a "65% year-on-year increase in the number of participants reporting that their organization lacks the technology to outpace the competition over the next twelve months."

EV Transition

An excerpt from the Indiana EV Product Report, highlights the impact of manufacturers, 'The automotive industry is amid a transition - replacing the Internal Combustion (ICE) engine-based cars with a new energy source – battery-powered Electric Vehicles (EV). Based on research from the EVP Commission, the possible U.S. market size for EVs goes from 1.45 million to 6 million vehicles by 2030, a significant opportunity, albeit highly variable, and a function of automaker choices.

Supply Chain Disruptions

The recent experience with the post-pandemic supply chain disruptions impacted almost all manufacturers. Although that blip may be in the rear-view mirror, the recent rerouting of ships around Africa due to Red Seas attacks demonstrates that supply chain disruptions are always possible with a global supply chain. In addition, there is always a threat of a dock worker labor dispute at major ports.

Workforce Shortage and Work Ethic

Most businesses are having trouble finding qualified workers. A report published by Rockwell Automation states "46% of manufacturers say that they lack the skilled workforce to outpace the competition over the next 12 months".

1.4 WHAT ARE THE BENEFITS OF A SMART FACTORY?

KEY COMPANY BENEFITS

01 ——

Achieve a competitive edge – in today’s business environment your competitors are not only nearby in the region, but also global.

02 ——

Improved quality and productivity while reducing costs resulting in increased profits.

03 ——

Increased customer satisfaction by improving on-time delivery and quality.

KEY EMPLOYEE BENEFITS

01 ——

Improved job security by increasing company sustainability from company benefits.

02 ——

Enhanced personnel development with exposure to smart factory technology, such as cross-functional employment opportunities.

03 ——

Improved working conditions, as many of the labor-intensive difficult tasks are performed by automation enabling workers to perform more knowledge-based tasks.

04 ——

Increased wages and increased opportunity for advancement.

1.5 SMART TECHNOLOGY

The purpose of this report is to provide you with a working knowledge of smart technologies, so you can have the confidence to adapt to this new global reality. However, it is important that smart technology is not the goal, but rather, the outcomes of successfully applied smart technology are desired.

These outcomes being principally deployed to:

- Enhance people's productivity.
- Innovate and automate processes.
- Improve product functionality and quality.

Holistic Approach

Steering corporate objectives using a TP3 Framework provides the elements of a holistic plan. Each of the three Ps are impacted by technology. Similarly, process impacts products and people as well as technology, and so on. Anticipating all the connections impacts the ability to steer business strategy thus delivering the required agility to succeed.

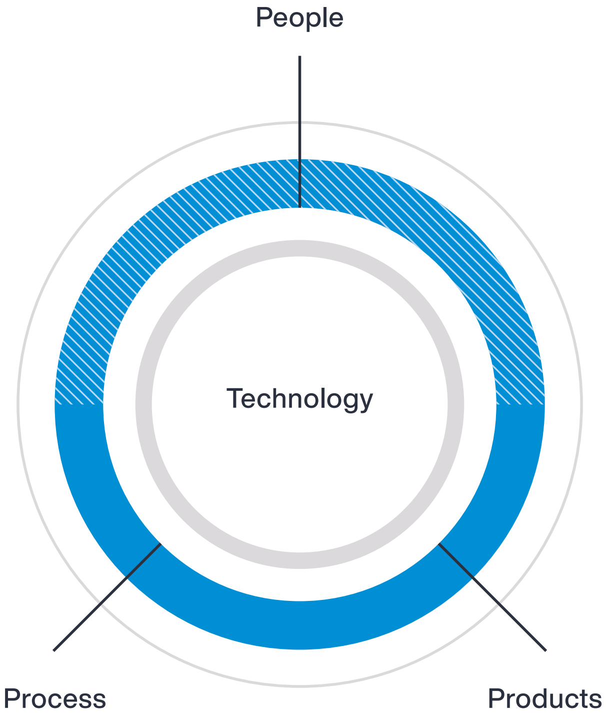


Figure 2 is an excerpt from the book, 'Smart Manufacturing: The New Normal, A TP3 Strategy.' where TP3 represents Technology, People, Product & Process.

Figure 2 - Steering using a TP^3 Framework.

Networks

Computer and communications networks enable computers, cell phones, IoT-enabled devices, and many other smart technologies to communicate with each other, company servers and internet cloud-based services.

5G cellular technology will have a major impact on the ability to transfer large amounts of data quickly.

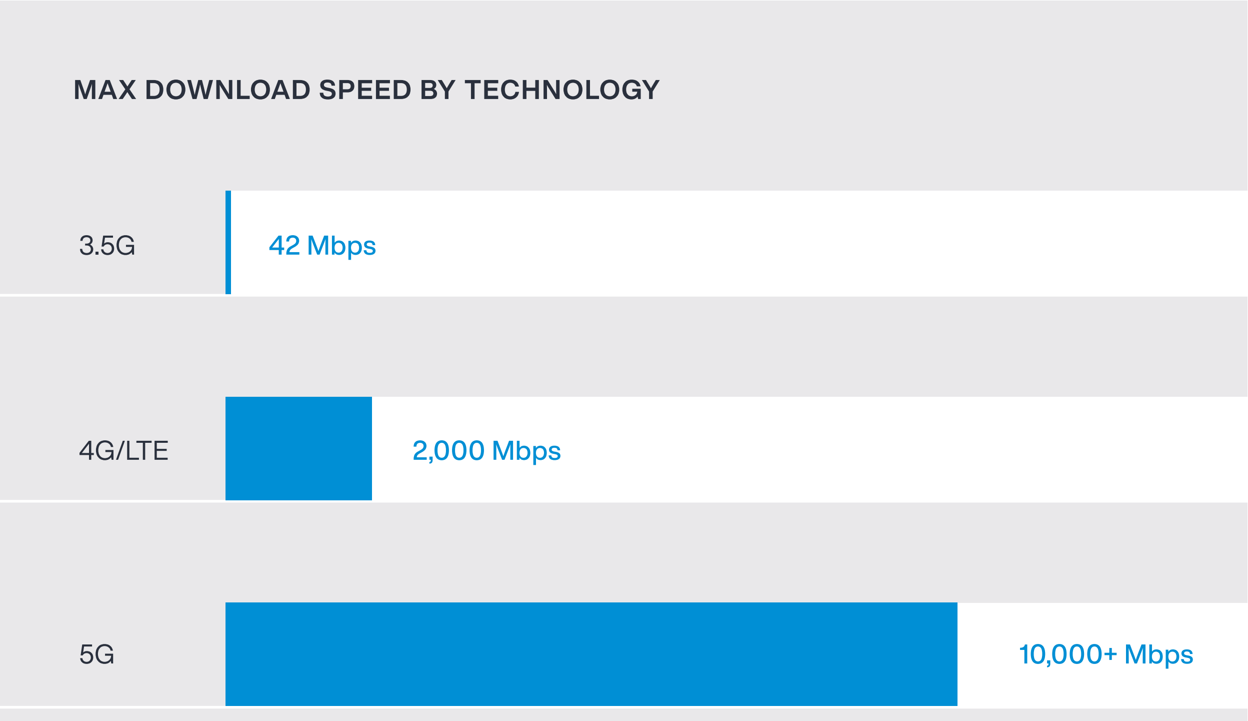


Figure 3 - Source: https://blog.hubspot.com/service/5g-customer-service

The Internet of Things (IoT) is not a new idea. Smart, connected devices that communicate with one another have been around for years. However, thanks to lower latency and improved reliability, 5G will allow for more of these devices to function on any one site.

IoT Sensors

IoT sensors are imbedded in almost everything including these examples:

Home: Alexa, cell phones, computers, refrigerators, smart doorbells, thermostats, security systems, AirTags, etc.

Factories: IoT empowers predictive maintenance and shop floor operations, allowing manufacturers to track all assets from resources in the production process to completed items in a warehouse.

Transportation: Personal vehicles, commercial vehicles, public transportation, boats, airplanes, trains, supply chain movement of goods.

Schools: Interactive whiteboards, temperature and environmental sensors, security cameras with computer vision (say, for detecting weapons), automated attendance tracking systems (see ID cards), etc.

Fitness & Health: Wearable fitness trackers, smart training gear, smart apparel/footwear, etc.

IoT Use Case in Manufacturing

Below is an example of how an air conditioning manufacturer uses IoT in its production cycle.

Factory: Both the manufacturing machines and conveyor belts have sensors that continuously send data regarding the machine health and the production specifics to the manufacturer (to identify issues during production). Then, after the AC is completed and before shipment, a bar code is attached to each product before leaving the factory. (Note: In the future, when IoT sensor cost is reduced to pennies, the bar code may be replaced with an IoT sensor like an AirTag). This identifier contains the product code, manufacturer details, special instructions, etc. Next, these products are packed and shipped to different retailers. In addition, IoT sensors are embedded in the final product to measure operational performance after installation.

Retailer: Each retailer scans barcodes to track the products received from different manufacturers, update inventory, check special instructions and track sales. The sales data is shared with manufacturers so they can replenish the product.

Consumer: Each air conditioner has embedded sensors that emit data regarding its health and temperature to the manufacturer in real-time. This data is analyzed continuously, enabling the manufacturer's support team to contact the consumer to assess the issue and schedule repair.

This is an example of how IoT sensors can be used in factories, by retailers, and by consumers.

Big Data/Data-Video Analytics

Big Data refers to large diverse sets of information that grow at ever-increasing rates that are being continuously collected from multiple sources. The data consists not only of traditional information that is found in spreadsheets and databases, but also includes: pictures, video, audio, etc. The results are billions of bits of data being collected daily. Thus, it is impractical for any human to analyze without the aid of sophisticated software, which will typically show meaningful information graphically.

In addition to data collected by IoT sensors, most manufacturers have two traditional software applications that process transactional data:

Enterprise Resource Planning (ERP): A joined-up software application that enables manufacturers to plan and operate production, finance, procurement, HR, and supply chain.

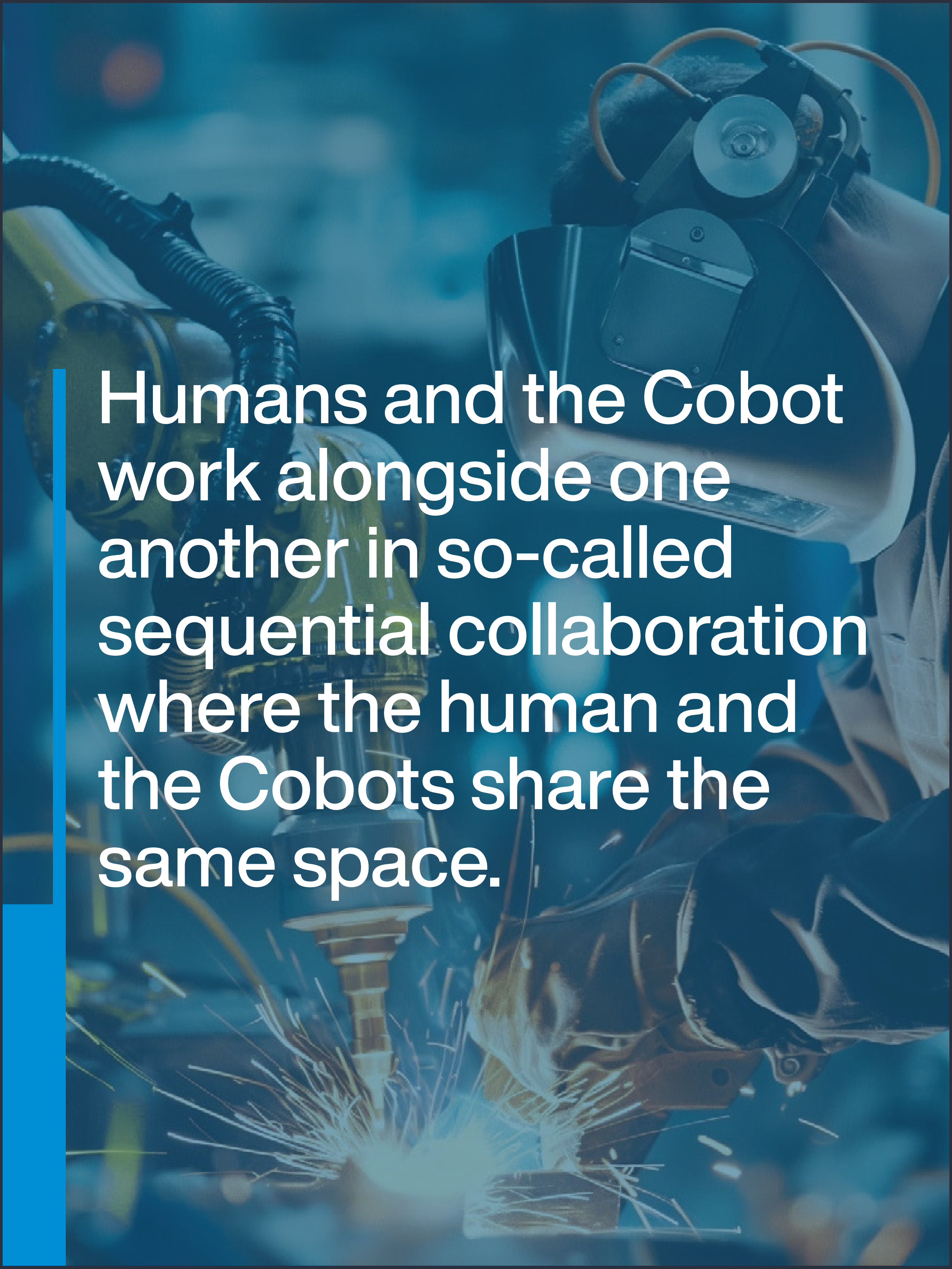
Manufacturing Execution Systems (MES): A software application that tracks and monitors the production process from beginning to end. It collects data related to production processes, results as well as quality.

Power BI and Tableau are software apps used to analyze traditional data stored in databases and excel spreadsheets. These productions can process massive amounts of data in real-time to create dashboards and alerts so that managers and plant floor workers can make smart decisions faster.

Video analytics software can analyze images to detect abnormal conditions. Vehicle backup cameras and other sensors are examples of everyday use. An example of use in a production environment is how GE., at its Lafayette, IN plant uses video analytics to perform final quality checks. After the airplane engine is completed, it is placed upright in a glass cage. Then a video camera scans the surface of each area of the engine by rotating around the engine layer by layer to compare the actual image to a digital version. Any deviation can be detected as the scan is completed, even a small screw missing or misaligned.

Audio analytics software can analyze audio signals to detect abnormal conditions. An example of how this is used in a manufacturing environment is in maintenance. IoT sensors can be affixed to plant floor equipment, motors, conveyers to record heat, vibrations, noise, etc. These audio recordings are analyzed in real-time to detect potential maintenance issues before a malfunction occurs. Thus, maintenance can be predictive instead of reactionary.

Billions of bits of data being collected daily. Thus, it is impractical for any human to analyze without the aid of sophisticated software



Humans and the Cobot work alongside one another in so-called sequential collaboration where the human and the Cobots share the same space.

Robots/Cobots

Traditional industrial programmable robots that will typically carry out lots of specific and complex tasks, producing car parts, doing some welding or other functions without human interaction. Usually these types of robots are located in safety enclosures and are programmed to do the same set of tasks over and over. Also, it is important to understand that these traditional robots are potentially dangerous to humans.

However, a Cobot stands for collaborative robot, meaning that both humans and robots are working together. To enable Cobots to work with and around humans, they are designed with padding, softer edges, and more sensors for approximation. Humans and the Cobot work alongside one another in so-called sequential collaboration where the human and the Cobots share the same space. But they do not work at the same time. So, one operation may be a human moving something and then the Cobot performing a function: maybe a spot weld or tightening a part.

An example of a human working with a Cobot is at the Cummins Colombus, IN plant. The worker uses an intelligent torque tool to tighten over 500 fasteners to seal the cover on a large bus battery. The torque gun is activated by a signal from an overhead camera. The camera sends a light signal to the next fastener to be tightened. When the worker affixes the torque tool to the highlighted fastener, torque is energized via a wireless signal from the camera, the proper torque is applied to tighten the fastener and the light turns green to confirm. The process is repeated until all 500-plus fasteners are tightened in the exact sequence as is designated by the engineers to ensure that the battery cover is sealed properly. This process is like playing 'Wack-a-mole.' It would be nearly impossible for the worker to remember the exact sequence because by design the pattern would require the worker to move about side-to-side and front-to-back.

Digital Twin

A digital twin is a digital representation that is not linked to an actual product by model and serial number. The product is usually one that is critical to monitor actual performance. A couple examples are GE 737 airplane engines and Ford EV batteries. The benefit of a digital twin is when data is collected in real-time from the actual version of the product.

In the case of GE airplane engines, data is collected as the engine is placed in service. This data includes not only the mechanical performance of the engine and maintenance activities but also environmental conditions such as: start/stop, speed, temperature, fuel, wind, dirt, bugs, birds, etc. As this data is collected, the digital twin is updated so that it reflects the current functionality of the actual engine. This image is compared to the design expectations for the specific engine so that any deviation for the expected performance or function can be detected.

The benefit is that unplanned maintenance can be identified and scheduled; emergency situations can be detected so that the airplane can be taken out of service to prevent a potential crash. In addition, the long-term reliability of the engine can be estimated to predict when an engine would be either replaced or overhauled. The efficacy of the pilot in non-stressing the engines, and so lengthening the service intervals, can also be used to improve pilot's performance.

Ford also is planning to utilize digital twins to monitor the performance of EV batteries. This will be especially valuable because there is not much historical information regarding the actual battery performance in various environmental conditions. In fact, recently it has been reported that EV batteries in Chicago were losing their charge faster in the cold temperatures than under normal temperatures and had issues in recharging. This is an example of the benefit of having real-time data uploaded to a digital twin that would identify weaknesses in the design and enable engineers to modify future design; they could make retrofit engineering changes to batteries in service. The point testing and simulation in a laboratory is limited and actual experience is invaluable.

Digital Supply Chain

A Digital Supply Chain (DSC) is a supply chain that leverages digital technologies and data analytics to guide:

- Decision-making
- Optimize performance, and
- Quickly respond to changing conditions.

At their core, DSCs are powered by the data produced by existing supply chains, which are stored in data in the cloud and analyzed for actionable insights.

They differ from traditional supply chains by:

- Leveraging the data produced by each step of the process to ensure efficient planning.
- Creating dynamic responses when unforeseen delays arise.

Key components of a successful digital supply chain are:

- End-to-end visibility: This component ensures that businesses have real-time visibility into their supply chain operations, from sourcing raw materials to delivering products to customers.
- Real-time data access: It enables businesses to access and analyze data in real-time, allowing them to make informed decisions and respond quickly to changes.
- Configuration level monitoring: This component involves monitoring and managing the configuration of supply chain systems and processes to ensure optimal performance.
- Top-level scope & content: It refers to defining the scope and content of the digital supply chain strategy, including identifying key objectives, and aligning them with business goals.
- Leveraging new technologies: This component involves adopting and integrating new technologies such as artificial intelligence, machine learning, and blockchain to enhance supply chain operations.

In addition to IoT and ERP technologies, there are three additional digital technologies that are transforming supply chain operations.

01

Warehouse Management Systems (WMS)

Warehouse Management Systems (WMS) is a set of policies and processes intended to organize the work of a warehouse or distribution center and ensure that such a facility can operate efficiently and meet its objectives.

02

Blockchain

Blockchain is a distributed ledger with growing lists of records (blocks) that are securely linked together. Although most people relate blockchain technology with Crypto-currency, blockchains are also used in manufacturing especially where traceability is critical. For example, where and when each component of a space shuttle was produced.

03

Remote Collaboration Platforms Supply Chains

Remote Collaboration Platforms Supply Chains is defined as two or more autonomous firms working jointly to plan and execute supply chain operations. Collaboration software is essential for manufacturers to visualize supply chains end-to-end and to identify potential supply chain issues quickly.

Business Example

Embracing No-Code App Development for Streamlined Operations

In the realm of modern technology, the term “apps” generates thoughts of easy-to-use programs on smartphones and efficient productivity tools like those found in Google and Microsoft Office suites. However, a less-explored domain lies in the creation of custom-designed apps, which enable companies to sidestep the expenses associated with traditional commercial app development and distribution.

This case delves into the shift towards no-code app development, a cornerstone of digital transformation. The Purdue Dauch Center is exploring methodologies and processes that empower businesses to craft tailored apps at minimal costs, reflecting on our past projects spanning diverse functionalities; from streamlining fork truck safety records to facilitating employee onboarding and material management, the versatility of these apps is remarkable.

What distinguishes no-code apps is their seamless integration with existing back-end systems, be it Outlook, spreadsheets, or Google Sheets. By establishing a structured data framework, transitioning from back-end to front-end becomes a matter of simple linkage, freeing designers to focus on user-experience rather than grappling with technical intricacies.

Individuals can begin this journey by meticulously examining the material information workflows, culminating in the creation of a cloud-based spreadsheet. This serves as the foundation for seamless integration with a chosen no-code app platform. Notably, platforms like No Code App and PowerApps by Microsoft, offer a plethora of templates catering to various industries and functionalities, expediting the development process. Whether populating pre-existing data for display or facilitating real-time data entry, no-code app platforms offer intuitive interfaces for both scenarios, requiring minimal training.

Real-world examples further illustrate the transformative potential of no-code apps. From automating safety inspections for fork trucks to streamlining employee hiring processes and material flow management, the applications are numerous and adaptable to diverse business needs.

Here are a few examples of the apps we have developed by utilizing the No Code App software:

1. Fork Truck Safety Inspection App

Imagine a scenario where a company operates 35 fork trucks, requiring daily safety inspections adhering to 5S standards. An app facilitates this process seamlessly. Users conduct thorough safety inspections, inputting data based on predefined safety criteria. Once all safety checks are completed and satisfactory, the app updates the company records for the day. If any maintenance issues arise, the app automatically generates work requests for the affected fork trucks. While notifications could be integrated directly into the app, we the developer for this app opted for a streamlined approach using macros within the spreadsheet.

2. Employee Hiring App

In another project, an app was developed to streamline the employee hiring and application process. This app captures essential data elements akin to a traditional written application. This information is then compiled and forwarded to the relevant hiring manager, expediting the recruitment process, and ensuring seamless communication.

3. Material Flow Tracking App

The third example app focuses on tracking material flow between departments. Data captured within the app is seamlessly extracted and forwarded to an ERP system via Excel uploads. This integration significantly streamlines inventory management processes, ensuring accurate and real-time records of on-hand inventory.

These examples underscore the versatility and effectiveness of our no-code app solutions in addressing various business needs, from safety compliance to HR processes and inventory management.

Key to embracing no-code app development is its accessibility and cost-effectiveness. With minimal knowledge barriers and an array of templates at disposal, businesses can swiftly transition from concept to a fully functional app. Moreover, the scalability and affordability of licensing options ensure sustained operational efficiency without breaking the bank.

No-code apps represent the accessibility of app development, empowering businesses of all sizes to harness the power of digital transformation. As managers navigate this landscape of innovation, please feel free to contact the Dauch Center regarding no code apps, our previously mentioned cases, or enhanced productivity in this space.

1.6 OBSTACLES

External Factors

Cybersecurity is one of the biggest risks. Bad actors are continuously attempting to hack into companies' networks to steal information and/or install ransomware.

Pandemic hopefully is in the rear-view mirror; however, there is no insurance it or something similar will not make a comeback, so companies need to be vigilant.

Workforce shortages are a major issue for most businesses, and this is a long-term phenomenon, so automation may be the only way to overcome the shortfalls.

Material Prices are continuing to increase even though the rate of inflation is subsiding, so companies need to focus on other cost-cutting measures to offset these cost increases.

Supply Chain Distribution has become unreliable and forced manufacturers to play defense and, in many cases, maintain higher levels of inventory to compensate for uncertainty.

Internal Factors

Deploying & integrating new technology is a challenge for many SMEs because they lack skilled engineers and IT professionals to keep pace with technology that is rapidly changing.

Product quality must be a high priority for all manufacturers to remain competitive.

Onboarding new employees is critical to improving retention and to developing a productive employee.

Worker retention/knowledge continues to be a major headwind for manufacturing companies. Frequent turnover not only disrupts operations, but also creates a knowledge drain.

Understanding data to improve the business is important to be able to make smart decisions. Too much data creates information pollution that overwhelms managers and causes confusion.

DIGITAL TRANSFORMATION OBSTACLES

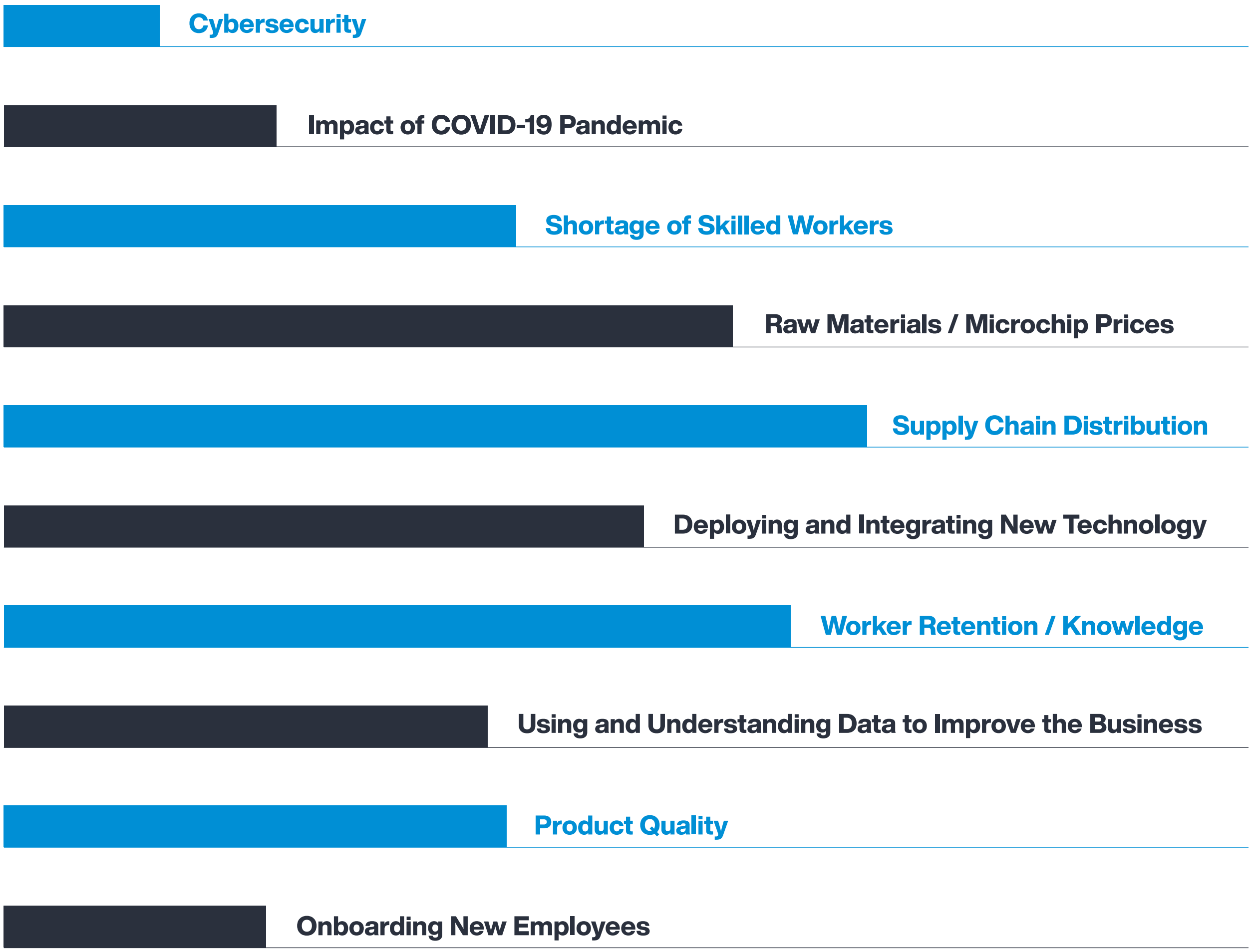


Figure 4 - Rockwell Automation: Eighth Annual Smart Manufacturing Report

Reid Paquin, Research Director, IDC Manufacturing Insights stated that “The manufacturing industry has maintained its rapid pace of change and disruption, making the ability to adapt a premium. Manufacturers have encountered many challenges in their efforts to become more resilient while maintaining efficiency, but one of the most cited issues are outdated/legacy systems. While the predictions highlighted touch upon many areas of the business, the main theme that can be tied back to is having the proper digital infrastructure in place.”

1.7 FUTURE TRENDS

01

Managing cybersecurity risks (e.g., ransomware, phishing) by installing cybersecurity software and ensuring it is updated frequently is the best way to fight cybersecurity risks. Although there is no way to prevent attacks, updating security software is the best defense.

02

Finding alternate materials or suppliers to meet demand will be critical to mitigate supply chain disruptions. In addition, Digital Supply Chain software will be necessary to monitor the supply chain and to enable companies to react in real-time to potential supply chain issues.

03

Digitizing business through software adoption and automation will be fundamental for manufacturing to prepare for digital transformation.

04

Shifting to cloud operations for data backup, business continuity, eliminating data/ communication silos, added cybersecurity protection, etc. is a necessity to fully participate in digital transformation.

05

Adopting software for automating processes and tracking/ quantifying sustainable practices is a high priority. However, it is important to not automate an inefficient process. Therefore, it is important for manufacturers to implement “Lean” best practices prior or in conjunction with installing automation.

06

Ensuring data accuracy for reporting and informed decision-making is imperative to ensure decision makers are presented with accurate information. Remember, just because information is created by a computer does not make it correct. “Garbage in = Garbage out.” Ensure that all software systems are fully tested before implementation.

TECHNOLOGY ADOPTION

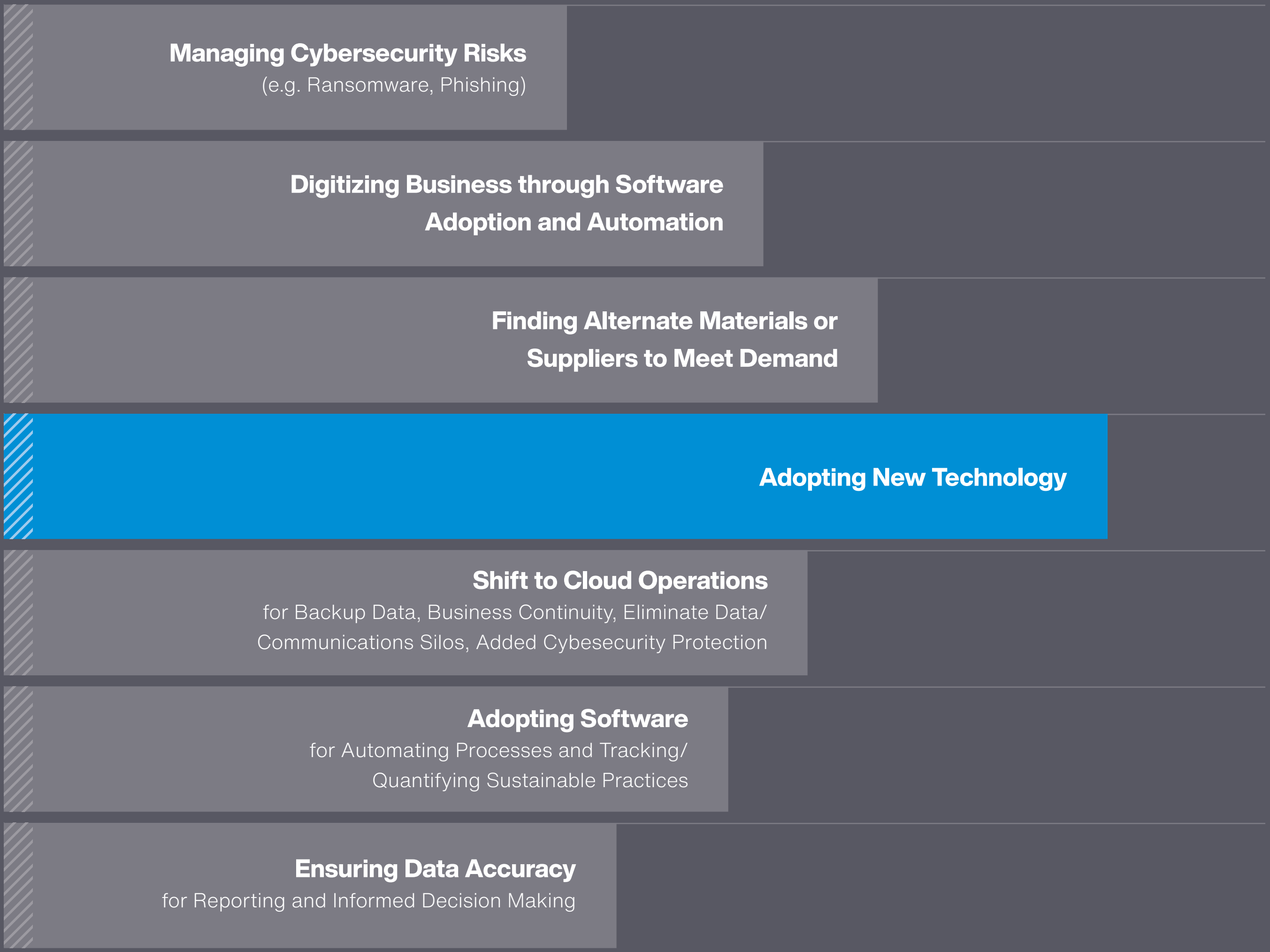


Figure 5 - Rockwell Automation: Eighth Annual Smart Manufacturing Report: Page 8

Bottom-line: the trend is clearly to adopt smart technology going forward and to upskill the workforce to implement/maintain technology, interface with smart equipment, and to understand how to utilize decision-making data.

1.8 RECOMMENDATIONS

What actions must manufacturers, government agencies, and technology companies take to facilitate and expedite the digital transformation of the US manufacturing industry to ensure that US manufacturers are competitive globally?

Manufacturers

Although each company is at a different stage on the journey to a smart factory, below are some key next steps on how to create a plan:

Assessment

Assess the current situation. Smart Factories rely on Internet of Things (IoT) technology to connect physical devices and enable data exchange to improve efficiency, productivity, and decision-making in manufacturing processes. This assessment developed by Purdue Dauch Center aims to evaluate a manufacturing company's readiness to implement IoT solutions. The assessment consists of three areas: Organizational Readiness, Operation Readiness, and Equipment Capability. The complete assessment survey is available at Purdue Dauch Center.

Metrics

Develop a set of metrics and establish a baseline so that progress can be measured as changes are being made. These metrics should include Quality, Productivity, Cost, and On-Time Delivery.

Vision

Create a blueprint of what constitutes a smart factory for each of the company's plants. In other words, one size does not fit all. Each plant is unique, and the smart factory design will vary depending on the types of products, equipment, size, etc. For each plant, create a CAD-type floor plan layout for current state and for future state and include a network infrastructure.

Roadmap

Develop a roadmap and budget on how to get to final vision. It is important that there is a well-thought-out plan before starting to make changes. Remember to streamline processes using "Lean" best practices prior to, or in conjunction with, installing automation.

LEADERSHIP ASSESSMENT

Is there strong leadership support and commitment to driving IoT Initiatives?

□ **None:** Not at this time

□ **Basic:** Have had internal discussions but no formal commitment

□ **In Process:** Commitment at mid-managment level but not at Senior Leadership level

□ **Implementing:** Commitment at leadership level but not communicated widely

□ **Advanced:** Strong leadership commitment and widely communicated

Leadership commitment is critical to a successful digital transition. Companies scoring low on this question can improve leadership commitment by educating management and/or contracting with a management mentor.

EQUIPMENT ASSESSMENT

Are your manufacturing machines and equipment capable of integrating with IoT devices or sensors?

□ **None:** None are capable or don't know capability

□ **Basic:** Some newer equipment has IoT but not connected to network

□ **In Process:** Have started to connect IoT to network and collect real-time data

□ **Implementing:** In-process of installing older equipment with IoT Devices (or replacing) and connecting to network

□ **Advanced:** Have implement IoT across plant, connected to IT, and using Data Analytics

Equipment assessment is a prerequisite to developing a digital transition plan. Companies that do not have the internal skills to complete this assessment can acquire these skills by training technical staff. If companies do not have a technical staff, then outside technical assistance may be the only option.

Government Agencies

Since it is important for the US to maintain a strong manufacturing base, the government agencies play a significant role in supporting and motivating manufacturers to develop a digital transformation strategy. Below are areas that governments both at a national and state level should consider:

Policies/Regulations

It is important to establish policies and regulations, especially regarding standards; however, it is also important to ensure that they are not too restrictive and costly to adhere to. In other words, do not make them too burdensome for businesses to comply.

Grants

Grants should be considered to establish regional Advanced Manufacturing Centers. These centers would consist of full-scale Smart Factories that would provide manufacturer's leaders, managers, and technical workers an opportunity to observe an actual working example of key smart technologies in a Smart Factory environment. In addition, workshops would provide workforce development opportunities for all levels of employees. Advisors would be available to assist manufactures with developing a strategic plan.

Incentives

Incentives should be provided to motivate manufacturers to purchase and implement smart technology. In addition, training and workforce development tax credits or other incentives could ensure that the workforce can function effectively in a smart factory.

Technology Companies Role

Digital transformation is a complex process that requires a lot of resources and expertise. Technology companies play a crucial role in this process by providing the necessary tools and services to help businesses transform digitally. The following is a list of technology areas that service companies can enable customer companies to be successful with their digital transformation:

- They can help businesses identify the right technologies to use and provide training, support, and maintenance services.
- Ensure that each vendor's technology is compatible and integrates seamlessly with the digital infrastructure.
- Minimize rapid technology obsolescence. Ensure there is long-term support for prior versions of technology to avoid the need for businesses to continuously upgrade. If it is necessary to upgrade to the latest version, make it as seamless and automated as possible.
- In addition, technology companies can help businesses integrate their existing systems with new technologies, such as cloud computing, artificial intelligence, and IoT.
- Assist businesses with ROI analysis to show how leveraging technologies can improve their operations, increase efficiency, and reduce costs.

- It is important to note that digital transformation is not just about technology. It also requires a change in mindset and culture, as well as a willingness to experiment and take risks. Therefore, technology companies need to work closely with businesses to ensure that they can achieve their digital transformation goals.
- Create a tiered pricing model to enable small businesses to adopt technology at a low entry point to reduce the barriers to entry.

Workforce Development

The Smart Factory needs to have an established work-culture where people feel valuable to maintain quality, safety, and positive attitudes to continuous improvement. Therefore, there is a need to address staff turnover and retention while creating pathways for those staff wanting and willing to develop and move with change and technology. Improvement projects and policies need to involve more staff, to create positivity about smart technology investments. Communication in manufacturing SMEs invariably needs to be improved to focus on the (certain delivery of) aspirational outcomes for workers at all levels when switching to smart technology. Some of the following can be seen as important though will depend upon the desired work-culture and local issues.

- Attractive, clean, well-lit workspaces and facilities.
- Onboarding and regular face-to-face follow-up support, including career/development reviews.
- Subsidies and schemes to reduce the cost of training in process (e.g., “Lean”), people (e.g., communication and feedback) and technology training.
- Move to receptive and rewarding mechanisms for employee suggestions, especially ones delivering success in safety, cost-savings, product quality and innovation.
- Training supervisors and shop-floor managers in facilitative communication and team building (since so many workers leave their manufacturing job to get away from their immediate manager, not, as sometimes stated, to move away from the business).

> **There is a need to address staff turnover and retention while creating pathways for those staff wanting and willing to develop and move with change and technology...**

Conclusion

The state of manufacturing is in a great era of transformation. There are a confluence of disruptions that require manufacturing leaders to rethink how they operate, to remain competitive in future.

The challenges of disruptions include:

- Digital Transformation is now a viable path for manufacturers because cost is rapidly decreasing. Technology is extremely modular so that technology can be deployed on a small scale initially. However, without a comprehensive blueprint and step-by-step roadmap, there is a risk that the result may be less optimum than expected.
- EV Transition is a major risk for almost all suppliers in the automotive sector. Even though recent headlines indicate the transition may take longer than initially forecasted, nevertheless it is still too much of a risk to be ignored. Designing and implementing a smart factory makes it more agile and easier to diversify into other products to maintain cash-flow and margins.
- Supply Chain disruptions are extremely unpredictable, so it is difficult to see them coming until it is too late to take mitigating action. This is where a digital supply chain is valuable to identify issues upstream, so that manufacturers can take mitigating actions such as: airfreight supplies and/or shift production to products not affected by disruption. In addition, visibility downstream through the distribution channels and retailers can improve demand forecasting, to improve production scheduling.
- Workforce disruption is impacting almost all employers, especially manufacturers. The workforce is aging which means that older, deeply knowledgeable workers, are retiring, but the younger workers are not so willing to work in manufacturing. Automation will reduce the need for workers, but also it can be a tool to attract younger workers because they are more enthusiastic about working with technology. In fact, a manager of a local manufacturing company commented, “Workers enjoy going home and telling children or friends about working with technology, especially, Cobots.”

Company leaders must prioritize supporting their workforce and develop smarter people and teams. The positivism for incremental change and communication of smart technology change is critical to success. There are many examples of workforce reluctance to support smart technology projects including actual sabotage and total reversal of project implementation.

In conclusion now is the time for Manufacturers, Government Agencies, and Technology Companies to work together to accelerate digital transformation and create more smart factories with smart people in the US. These actions will not only ensure US manufacturers are competitive globally, but will also provide a more adequate level of national security by having a strong and sustainable US manufacturing base.

Navigating the Impact of Smart Factories on Labor Dynamics

A fully functional smart factory often evokes thoughts of machine-generated intelligence. However, while investing in digital technologies, it is essential not to overlook the importance of human ingenuity and labor that have driven manufacturing forward for thousands of years.

A smart manufacturing strategy must include investment in upskilling and reskilling to ensure that your business indeed is utilizing all its assets. This starts with leadership prioritizing "smart people development" – motivating, empowering, and coaching their teams to embrace new technologies, adapt to evolving processes, and drive continuous innovation.

Workforce shortage will continue to be a challenge if we do not focus on the ethics behind how we see, hear, and understand our employees. Benefits of a smart factory for employees can look like increased wages and increased opportunities for advancement. But this only becomes clear if there is a long-term strategy and investment for upskilling and reskilling.

Additionally, success in the ever-evolving digital realm requires stronger connections between our people and technology, as well as among themselves. Data transforms into valuable information when paired with effective decision-making processes. Elevating the workforce to enhance their decision-making skills is crucial for harnessing the full potential of your data.

What will collaboration between employees and managers look like in the future? As we adapt to working alongside cobots, it is crucial to learn how to co-exist with both machines and each other in this new digital environment. Success will depend on agility and a balance between leveraging data and using soft skills, such as decision-making and intuition, for effective outcomes in a digital supply chain.

To successfully integrate smart manufacturing into your entire culture, focus on these basics: Communication, Involvement, Co-Design, and Inclusive Change Management. Understand the mindset of your teams before introducing changes; this ensures more effective skill development and reduces doubt and uncertainty. A robust cultural strategy alongside digital transformation is essential for sustainable implementation and long-term success.

Guiding Principles for Integrating Smart Manufacturing

1. Investment in People and Technology

For a fully functional smart factory, it's essential to invest in both digital technology and the workforce. Upskilling and reskilling employees are crucial to utilize all assets effectively.

2. Leadership and Workforce Development

Leaders must focus on motivating, empowering, and coaching their teams. Effective people development involves connecting workers better with technology and each other at various operational layers.

3. Data-Driven Decision Making

Elevating workforce decision-making skills is vital. Data only becomes valuable information when the right decision-making processes are applied, highlighting the importance of training in data interpretation and use.

4. Workforce Ethics and Benefits

Addressing workforce shortages requires ethical consideration of how employees are perceived and treated. A long-term strategy for upskilling and reskilling can lead to increased wages and advancement opportunities, benefiting both the organization and its employees.

5. Cultural Integration and Change Management

Integrating smart manufacturing into the company culture involves clear communication, employee involvement, and designing changes collaboratively. Understanding team mindsets before introducing changes ensures more effective skill development and reduces uncertainty. A culture strategy alongside digital transformation is key to sustainable success.

Key Action Items

01

Enhance Supply Chain Security

Strengthen infrastructure and logistics networks to support a resilient supply chain. Implement policies that address potential disruptions, such as labor disputes or geopolitical conflicts, and promote domestic manufacturing to reduce dependency on global supply chains.

02

Embrace Digital Transformation

Develop and implement a strategic roadmap for digital transformation to stay competitive. Invest in smart factory technologies to enhance productivity, quality, and customer satisfaction. Collaborate with technology partners and seek government incentives to support digital upgrades.

03

Plan for the EV Transition

Proactively prepare for the shift from ICE to EV by aligning your production capabilities and supply chains with the evolving automotive landscape. Leverage industry forecasts and collaborate with automakers to capture the opportunities presented by the growing EV market.

02

Industrial Artificial Intelligence

Jay Lee

Clark Distinguished Professor,
Director of Industrial Artificial Intelligence Center
Department of Mechanical Engineering
University of Maryland

UNIVERSITY OF
MARYLAND

2.1 INTRODUCTION

Artificial Intelligence (AI) is one of the most powerful technologies of our time. It represents a branch of cognitive science that allows humans to discover numerous intelligent methods for modeling our sensing and reasoning capabilities. However, industrial AI is a disciplined approach that empowers engineers to systematically create and implement AI algorithms, achieving repeatable and consistent success. This chapter explains the application of Industrial AI in smart manufacturing and maintenance to demonstrate the efficacy of Industrial AI in enhancing operational efficiency, reliability, and productivity. The chapter also highlights the pivotal role of multidimensional learning and transfer learning in evolving Industrial AI, emphasizing its potential to address the unique challenges of industrial perspectives. Lastly, the challenges advocate for a collaborative effort between academia and industry to navigate the complexities of data management, cybersecurity, and model interpretability, ensuring the robust, secure, and effective deployment of Industrial AI technologies.

2.2 BASIC PROBLEMS IN INDUSTRY

The race to achieve innovation leadership in smart manufacturing is accelerating among companies in Europe, the U.S., and Asia. This industry is facing a transformation, propelled by technological advancements that enable the digitization of factories. The Fourth Industrial Revolution is able to create significant financial and operational benefits, enhancing productivity and customer satisfaction. The journey towards Industry 4.0 began with boosts in productivity, and was quickly followed by enhancements in flexibility, quality, and speed.

Flexibility is realized through interactions between machines and humans, creating a dynamic, on-demand production system that can adapt on the fly.

Quality is improved and can be facilitated by monitoring plants in real time and implementing just-in-time maintenance. The deterioration of manufacturing equipment and tools compromises product quality and lowers productivity by increasing the frequency of unplanned downtime. Thus, intelligent prognostic and health management (PHM) tools become crucial for just-in-time maintenance, ensuring the delivery of high-quality products, reducing unplanned downtime, and boosting customer satisfaction.

Speed is achieved by enhancing connectivity among various sectors within the manufacturing process, affecting the entire product lifecycle. The integration of data across companies, vertically and horizontally, fosters transparency and unity among companies, departments, and functions, significantly enhancing manufacturing efficiency.

Driven by these objectives, both in the short and long term, the realization of Industry 4.0 continues to be a major focus for industry leaders across the manufacturing sectors. Yet, the rapid adoption of these technologies on a large scale has been a challenge for many manufacturing sites. It is essential for solving three major problems, as delineated: discipline problems, system problems, and intrinsic problems.

Discipline problems comprise aspects like workforce competency, the organization's culture, and management capabilities. Japan serves as a prime example due to its skilled workforce and efficient mechanisms for transferring knowledge that can cultivate a strong organizational culture.

System problems relate to equipment, systems, and processes. Germany demonstrates exceptional prowess by leveraging meticulously crafted equipment, process standards, and superior equipment design and manufacturing capabilities for knowledge transfer.

Intrinsic problems involve customer value creation. The United States leads by innovating business models and implementing technology, utilizing collaborative innovation based on intellectual property, domain data, and continuous service innovation for knowledge transfer.

Industrial Artificial Intelligence (Industrial AI) emerges as a powerful solution to these challenges, offering significant opportunities for manufacturing enhancement due to improving the quality, structure, and essence of manufacturing processes. By standardizing workflows through data, Industrial AI enables rapid accumulation of experience and facilitates efficient knowledge transfer. This utilization of data not only makes hidden issues in manufacturing systems evident but also promotes transparent management of equipment health, stabilizes process parameters, and optimizes overall efficiency.

Moreover, data acts as a conduit for augmenting user value, enhancing the functionality and reliability of products and equipment, improving operational efficiency, and strengthening enterprise sustainable profitability. Therefore, the integration of Industrial AI into manufacturing addresses these three fundamental problems by leveraging data-driven insights and automation. It ensures that discipline problems are mitigated by enhancing workforce competency and management capabilities through intelligent insights. System problems are resolved by improving equipment design, manufacturing processes, and system integration, making the entire manufacturing process more transparent and efficient.

Lastly, intrinsic problems related to customer value creation are addressed by innovating business models and technologies that lead to collaborative innovation and continuous service improvement. In essence, the industry's need for AI intervention is underscored by these challenges, highlighting Industrial AI's role as a critical enabler of manufacturing excellence.

This industry is facing a transformation, propelled by technological advancements that enable the digitization of factories.

2.3 THE PURPOSE OF INDUSTRIAL AI

The concept of Industrial Intelligence systems is interpreted in several ways across academic and industrial sectors. Attempts to define Industrial Intelligence as a distinct technology or solution often miss essential questions such as the specific type of intelligence needed for industrial settings, the unresolved problems and challenges where existing methods fail to address, and the role of AI in bridging these gaps. Moreover, the scope of Industrial AI should extend beyond showcasing the skills of data scientists in transforming traditional industrial models. It should focus more on identifying and solving hidden problems within industrial ecosystems.

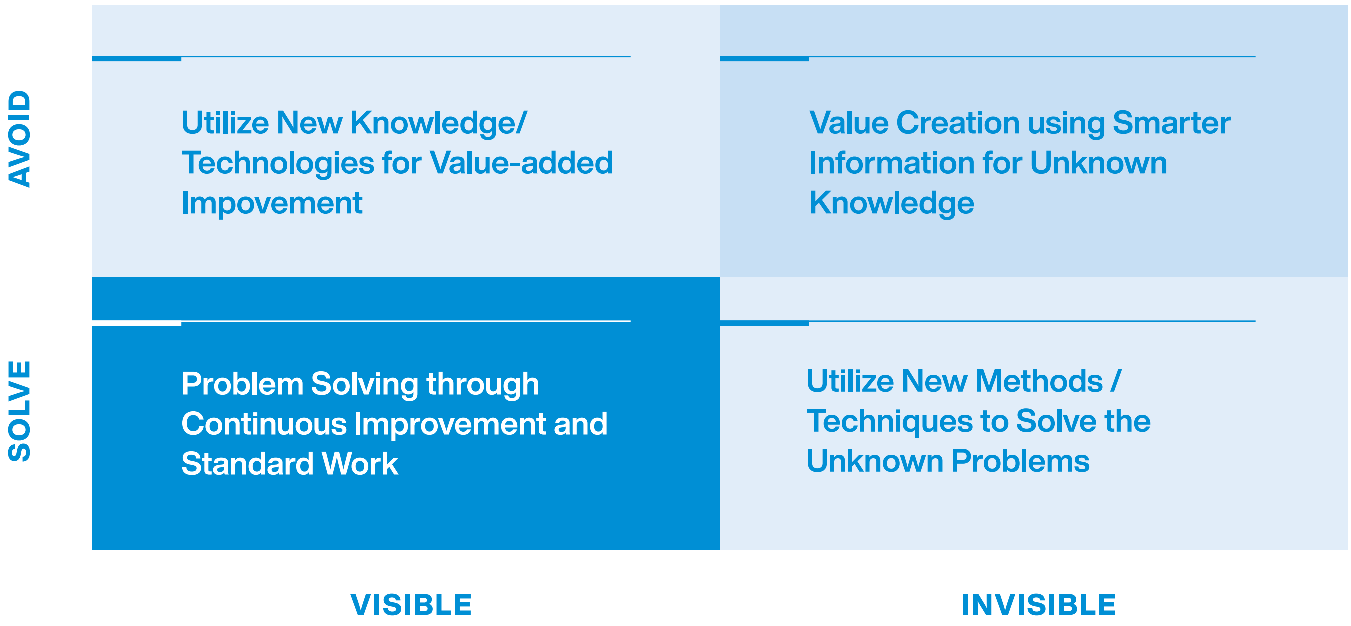
Industrial AI is not just about applying general AI technologies in industrial environments. The unique characteristics of the industrial setting, which include fragmentation, individualization, and specialization of challenges, require a comprehensive approach that blends computer science, AI, and domain-specific expertise. Unlike traditional rule-based or mechanistic models, the real power of data-driven Industrial Intelligence comes from its predictive analytics capabilities. These are built on insights and evidence gathered from data, enabling the development of intelligent management tools for previously unrecognized challenges. It also helps in uncovering complex interdependencies, thus generating a wealth of new knowledge, and promoting the development of an intelligently evolving system that improves over time.

The unique characteristics of the industrial setting, which include fragmentation, individualization, and specialization of challenges, require a comprehensive approach that blends computer science, AI, and domain-specific expertise. Unlike traditional rule-based or mechanistic models, the real power of data-driven Industrial Intelligence comes from its predictive analytics capabilities.

Manufacturing challenges can broadly be categorized into two distinct areas as illustrated in Figure 1: the visible and the invisible. Examples of visible issues include machine breakdowns, reduced production yield, and a decline in product quality. Conversely, invisible problems are those like machine wear, component degradation, and insufficient lubrication. Typically, clearly defined issues such as equipment breakdowns, quality lapses, and productivity shortfalls are addressed through continuous improvement and standardized practices, representing the traditional approach to manufacturing (located in the lower left quadrant). In pursuit of a competitive edge, modern manufacturers are increasingly leveraging AI algorithms.

This strategy is aimed at designing, producing, and delivering high-quality products that meet customer expectations more rapidly than their rivals, thus focusing on preempting problems (situated in the upper left quadrant). Recent initiatives by numerous firms have resulted in the innovation of new methods and techniques specifically targeting invisible challenges (identified in the lower right quadrant). The integration of an Industrial AI-driven methodology promises to unlock new possibilities for value creation within smart manufacturing, particularly in dynamic and unpredictable environments (highlighted in the upper right quadrant). A comprehensive adoption of Industrial AI's core components not only facilitates the resolution of visible issues but also helps in circumventing the invisible ones.

Industrial AI plays a pivotal role in realizing the three Ws of smart manufacturing: Work Reduction, Waste Reduction, and Worry-Free Manufacturing. The concept of 'Worry' in modern manufacturing systems often stems from invisible issues such as poor product quality, customer dissatisfaction, or a downturn in business. To tackle these challenges effectively, it is crucial to deploy industrial AI technologies through a structured approach. Moreover, the goals of diminishing workloads and waste can be met by pinpointing the visible elements of these issues and proactively addressing their potential future impacts with the aid of adaptable AI modules.



	VISIBLE	INVISIBLE
AVOID	Utilize New Knowledge/ Technologies for Value-added Impovement	Value Creation using Smarter Information for Unknown Knowledge
SOLVE	Problem Solving through Continuous Improvement and Standard Work	Utilize New Methods / Techniques to Solve the Unknown Problems

Figure 1 - Visible and invisible problems in industrial systems

2.4 DIFFERENCES BETWEEN AI AND INDUSTRIAL AI

The distinctions between AI in general and Industrial Artificial Intelligence are multifaceted, encompassing not merely the sphere of application but also diverging in terms of functional prerequisites and algorithmic approaches. Prior to delving into these differences, it is imperative to delineate the definitions of both terms. AI represents a branch of cognitive science characterized by extensive research into imaging analysis and machine vision, natural language processing, robotics, and machine learning, among other areas. Despite its profound potential, AI is often shrouded in mystique, frequently criticized for its lack of tangible evidence to substantiate its efficacy, repeatability, and financial return on investment within an industrial context.

Conversely, Industrial Artificial Intelligence is defined as a disciplined approach dedicated to the development, validation, and swift deployment of machine learning algorithms tailored for industrial use cases, ensuring sustained performance. This domain focuses on engendering intelligent systems tailored to industrial applications, embodying systematic development, rapid deployment, and sustainability. Owing to its emphasis on convergence and efficiency, Industrial AI plays a pivotal role in enhancing energy efficiency, safety in industrial production and equipment, transportation safety, and machinery stability. Its applications are predominantly targeted towards industrial and manufacturing equipment, transportation, the energy sector, production apparatus, and automation processes (refer to Table 1).

	AI	INDUSTRIAL AI
Definition	A trial-and-error judgement-driven technology applied to NLP, image processing, automatic reasoning, robotics, and so on. It can be used in lots of areas like medicine and business. However, it has not really worked out well in engineering yet.	In the industrial domain, AI applications are deployed by training and methodologies characterized by their rapidity, systematic approach, and sustainability. This framework ensures that a diverse range of users can employ the tools effectively to achieve uniform outcomes, thereby contributing to the progression of AI standardization
Function	Divergent and opportunity-driven situations (e.g., autonomous driving, economy sharing, and facial recognition)	In situations where we aim to get better and more efficient, we start with what we have and try to make it better in several ways. This includes making production faster and better quality, using less energy to save money, making machines more reliable, and making cars safer
Application Areas	Social networks, financial sector, medical industry, among others	Multiple industrial applications include Industrial equipment and manufacturing, power grids, power generation equipment, transportation and logistics, healthcare systems, and so on
Algorithms	Machine learning, deep learning	Non-traditional machine learning (i.e., Topology, domain adaptation, similarity-based learning), Deep learning, broad learning, fuzzy learning, augmented learning

Table 1 - Differences between AI and Industrial AI

Figure 2 delineates the distinctions among Industrial AI, machine learning, expert systems, and the realm of human expertise. Expertise, in this context, denotes the proficiency acquired by technicians through extensive hands-on experience. An illustrative case is the diagnosis of faults in rotating machinery, where seasoned experts can accurately identify and pinpoint issues solely by auditory cues. Nonetheless, the transference of such expertise presents formidable challenges, with a significant portion of this knowledge at risk of being lost upon the departure of experienced personnel, thus posing a threat to the sustainability of problem-solving capabilities within enterprises. Moreover, this expertise is inherently limited in addressing non-apparent issues, exemplified by the inability of even the most skilled experts to precisely evaluate the current health status of equipment. Expert systems, anchored in domain-specific knowledge and structured around a knowledge base and inference mechanisms, face challenges in adapting to uncertainties prompted by environmental and operational shifts. Enhancements in system performance necessitate regular updates. Compared to these traditional methodologies, AI and machine learning-based systems exhibit a substantial enhancement in problem-solving accuracy and possess remarkable adaptive learning capabilities. Nonetheless, these systems often demonstrate limited robustness under variable working conditions and with heterogeneous data sets. Anticipated advancements in Industrial AI, underpinned by multidimensional and systematic transfer learning approaches, are expected to yield consistent improvements in system performance.

COMPARISONS OF EXPERT EXPERTISE, EXPERT SYSTEMS, AI & INDUSTRIAL AI

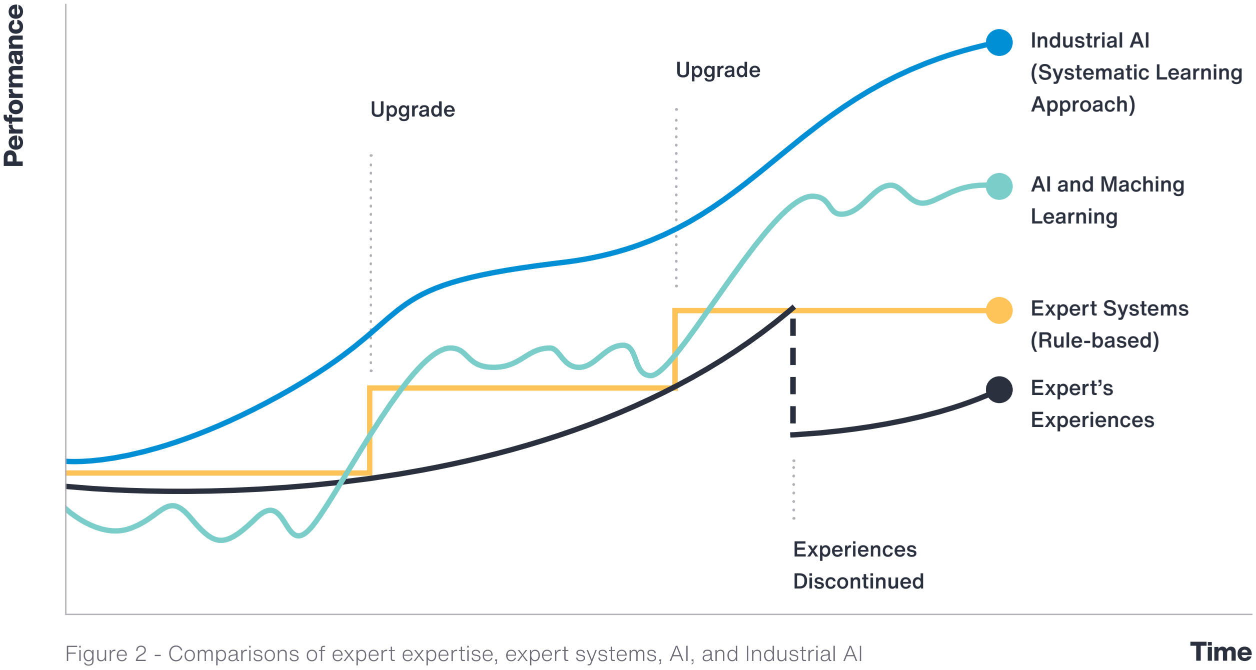


Figure 2 - Comparisons of expert expertise, expert systems, AI, and Industrial AI

2.5 DEFINITION AND MEANING OF INDUSTRIAL AI

Industrial Artificial Intelligence represents a significant shift in the operational paradigms of various industries, heralding a new era of efficiency, reliability, and productivity enhancement. This transformative potential is primarily driven by the growing need for predictive maintenance, streamlined production processes, and the optimization of manufacturing systems. The inception of Industrial AI emerged from the recognition of the need for a systematic integration of AI technologies within industrial frameworks. This approach is distinct from the broader applications of traditional AI, which span a wide range of uses from autonomous vehicles to virtual assistants. Industrial AI is specifically tailored to meet the unique requirements and challenges inherent to industrial contexts, focusing on enhancing operational efficiency, reliability, and productivity in ways that directly address the complexities of these environments.

At its core, Industrial AI encompasses the deployment of machine learning algorithms and AI techniques to refine industrial operations. This involves a rigorous process of developing, validating, and deploying such technologies to address real-world industrial quandaries, thereby acting as a conduit between academic research findings and practical industrial applications. The essence of Industrial AI transcends the mere repurposing of general AI technologies; it necessitates a profound amalgamation of AI with domain-specific acumen to tackle the peculiar challenges posed by industrial systems. The primary objective of Industrial AI is to bolster the performance and reliability of industrial mechanisms through the application of predictive analytics. This not only facilitates a reduction in operational expenditure but also augments efficiency across the board. By harnessing a myriad of data sources, including sensor outputs and historical records, Industrial AI models are capable of forecasting equipment failures, streamlining maintenance schedules, and enhancing overall plant functionality. Such a systematic approach guarantees the sustainability and consistent value delivery of Industrial AI solutions over time.

Industrial AI requires a large amount of data with which to train its algorithm. Companies that have invested in industrial digitalization will already have a steady volume of information streaming from their assets. The reality is that most of the data sets are useful but might not be useable for machine learning due to the lack of background, baseline, and its brokenness of the datasets. According to a recent study report from National Academy of Engineering, the key issues to successfully develop and deploy AI for industrial applications including the lack of quality data as well as lack of systematic approach in developing and validating AI. In addition, AI trustworthiness and lack of standards are adding risks for AI in its applications.

The current challenge is to develop a systematic discipline which focuses on developing, validating, and deploying various AI methods and machine learning algorithms for industrial applications with sustainable performance, scalability, and security. Combined with the state-of-the-art sensing, communication and big data analytics platforms, a systematic Industrial

AI methodology will allow integration of physical systems with computational models with an integrated learning platform to address the 3D issues (data, discipline, and domain) to transform from the common disciplines in traditional AI and machine learning to develop capabilities to strengthen interdisciplinary capabilities in diversified engineering systems (Figure 3).

AN INDUSTRIAL AI SYSTEM

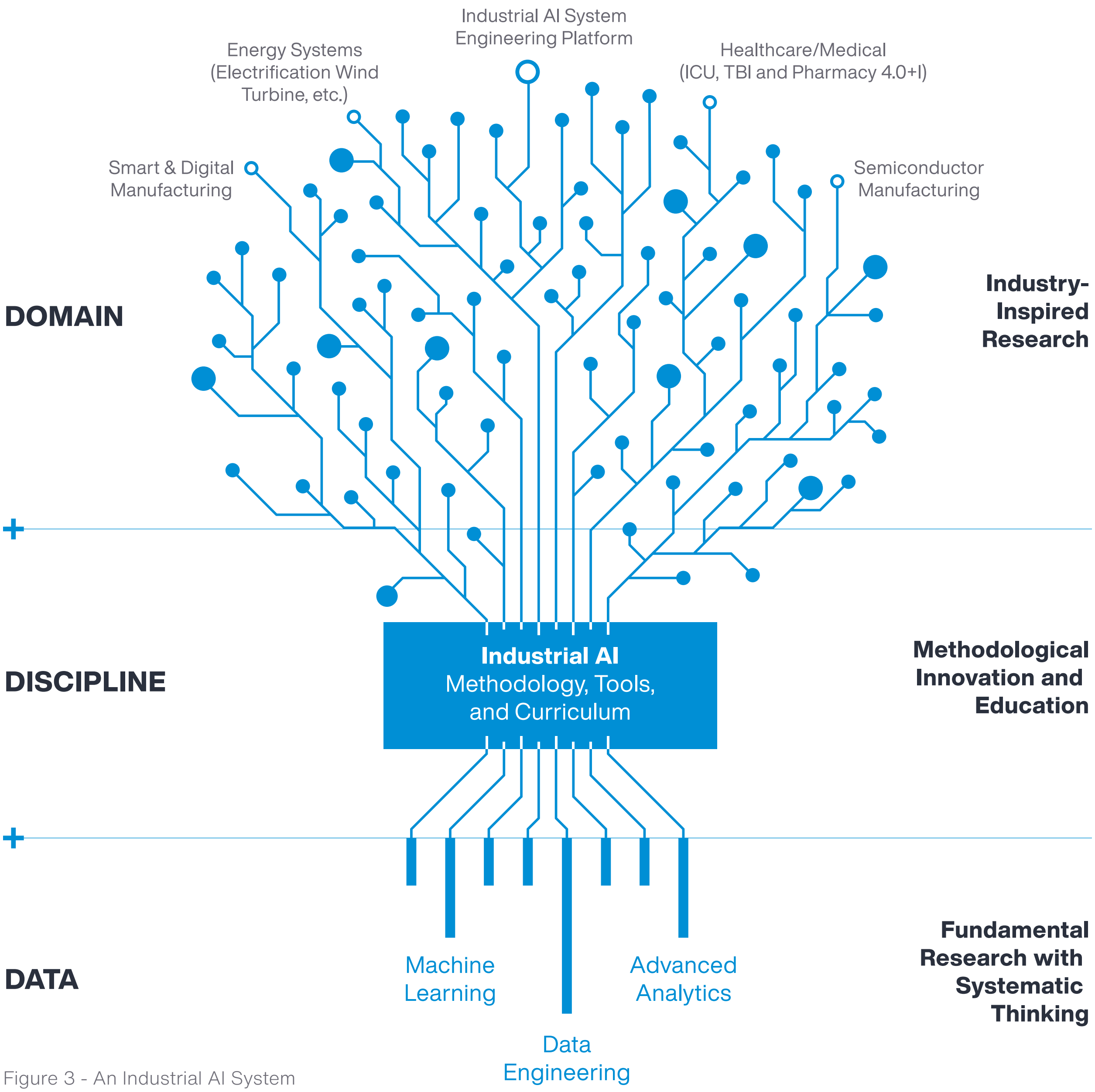


Figure 3 - An Industrial AI System

2.6 KEY ELEMENTS IN INDUSTRIAL AI: ABCDE

The foundation of Industrial Artificial Intelligence is built upon five crucial elements, succinctly referred to as ABCDE. These elements collectively represent the cornerstone in the development and application of Industrial AI technologies, which enable the transformation of industrial processes into intelligent, efficient, and predictive systems.

Analytics forms the core of Industrial AI, embodying the methods and technologies used to analyze data and extract meaningful insights. This element incorporates the application of machine learning algorithms, statistical models, and data processing techniques to discern trends, behaviors, and outcomes within industrial operations. Through analytics, industries can advance from descriptive analysis to predictive and prescriptive insights, enabling proactive decision-making and process optimization.

Big Data technology provides vast and varied datasets essential for the functioning of Industrial AI. Generated in large volumes from sensors, machines, and operational processes, this data is characterized by its volume, velocity, and variety. It is instrumental for training AI models, identifying patterns, and facilitating informed decisions. Big Data technologies are pivotal for the storage, processing, and analysis of industrial data, ensuring the effective operation of Industrial AI systems and the delivery of real-time insights.

Cloud or Cyber Technology delivers the necessary infrastructure and platform for deploying and accessing Industrial AI applications. It supports the scalability, flexibility, and computational power needed to manage Big Data. By offering a centralized platform for data storage, analytics, and application deployment, cloud technology integrates AI into industrial processes and aids in the development of cyber-physical systems. These systems allow for the monitoring, control, and optimization of physical industrial processes through cyber technologies.

Domain Knowledge is a vital component for the successful application of Industrial AI. It entails a deep understanding of the specific needs, challenges, and complexities of the industrial domain where AI is implemented. This knowledge guarantees that AI solutions are practical, relevant, and capable of solving real-world industrial issues. Domain experts play a key role in the development of Industrial AI applications, ensuring they are aligned with the realities of industrial operations and meet the sector's specific requirements.

Evidence encompasses the data and empirical findings that corroborate the effectiveness and precision of Industrial AI models. Collecting and analyzing performance data is crucial for validating that AI applications meet their intended goals, such as enhancing efficiency, minimizing downtime, or improving quality. Evidence is fundamental for establishing trust in Industrial AI systems, demonstrating their value, and promoting their adoption within the industry. Additionally, it is instrumental in the continuous enhancement and refinement of AI models, ensuring their relevance and efficacy over time.

The ABCDE framework outlines a comprehensive strategy for developing and deploying Industrial AI systems. By emphasizing these key components, industries can leverage AI to revolutionize their operations, achieve significant efficiencies, and secure a competitive advantage in the digital and automated industrial landscape. The successful integration of these elements necessitates a collaborative effort among data scientists, domain experts, and industrial practitioners, ensuring that Industrial AI solutions are not only technologically sophisticated but also practically viable and deeply rooted in industrial reality.

2.7 CYBER-PHYSICAL SYSTEMS (CPS) FRAMEWORK

The integration of Cyber-Physical Systems (CPS) and the strategic implementation of the 5C architecture are pivotal for the advancement of Industrial Artificial Intelligence (AI). This chapter delves into the CPS framework, the enabling technologies that support it, and the role of CPS in facilitating Industrial AI solutions, emphasizing the operationalization of the 5C architecture within industrial settings.

Cyber-Physical Systems (CPS) embody the convergence of physical industrial processes with advanced cyber technologies. This integration enables the monitoring, control, and optimization of industrial operations through real-time data analytics and AI-driven insights. CPS serves as the foundational framework for deploying Industrial AI, allowing industries to leverage computational intelligence to enhance efficiency, productivity, and adaptability in an increasingly digital world.

The 5C architecture outlines a systematic approach to implementing CPS in industrial environments, facilitating the gradual integration of Industrial AI across various operational layers. The architecture comprises five key components, each addressing specific aspects of CPS integration:

Connection: Establishes the data infrastructure, enabling seamless data collection from sensors and devices across the industrial ecosystem.

Conversion: Transforms raw data into actionable insights through preprocessing and advanced analytics, setting the stage for intelligent decision-making.

Cyber: Develops a digital twin of the physical system, offering a virtual platform for simulation and optimization without impacting actual operations.

Cognition: Employs AI and machine learning algorithms to analyze data, generating strategic decisions based on comprehensive insights.

Configuration: Applies the derived insights to reconfigure or adjust physical processes, optimizing performance and efficiency in real time.

Several key technologies enable the realization of CPS and the 5C architecture. The Internet of Things (IoT) links physical devices and machinery, enabling efficient data collection and communication. Big Data Analytics processes and interprets large data volumes, generating insights that inform decision-making. Cloud Computing provides the necessary

computational resources, data storage, and AI services, supporting the cyber dimension of CPS. In particular, Machine Learning and AI fuel the cognition component, facilitating predictive analytics and intelligent automation.

CPS significantly influences the deployment of Industrial AI by offering a coherent framework for merging digital technologies with physical industrial workflows. Through this framework and the 5C architecture, industries can achieve real-time monitoring and control, reducing downtime and boosting operational efficiency. Predictive maintenance, driven by AI, anticipates maintenance needs, reducing costs and enhancing productivity. Strategic decision-making, enriched by AI and analytics, fosters accurate, data-based strategies adaptable to evolving operational circumstances. Lastly, by leveraging CPS and Industrial AI, companies can quicken innovation, improve product quality, and secure a competitive market position.

The synergy of the CPS framework, the 5C architecture, and pivotal enabling technologies plays a vital role in the progression of Industrial AI within the manufacturing sector. This holistic strategy not only elevates operational efficiency but also spurs innovation, ensuring industrial competitiveness in the face of rapid technological evolution. Embracing CPS and the principles of the 5C architecture empowers industries to overcome the hurdles of digital transformation and seize the opportunities Industrial AI presents.

2.8 DEVELOPING AI TALENTS

To nurture new breeds of industrial AI engineers, there is an urgent need to accelerate AI talent development. Industrial AI Data Foundry is a data hub to host different datasets from real-world industrial problems to train engineers to apply AI to solve problem systemically. These dataset covers a broad range of manufacturing and engineering systems including automotive, aerospace, semiconductors, and industrial automation, etc. The training of industrial AI talents can use the 4Ps (Figure 4) approach (namely principle-based, practice-based, problem-based, and professional-based learning). These abilities need to be continuously cultivated in their work and encourage students to gradually grow into industrial AI leaders.

In smart manufacturing, students will learn how to harness the power of Industrial AI to gain insights into the invisible relationship of the operation conditions and further use that insight to optimize their uptime, productivity, and efficiency of their operations. In terms of predictive maintenance, Industrial AI can detect incipient changes in the system and predict the remaining useful life and further optimize maintenance tasks to avoid disruption to operations.

4P APPROACH FOR INDUSTRIAL AI TALENT DEVELOPMENT

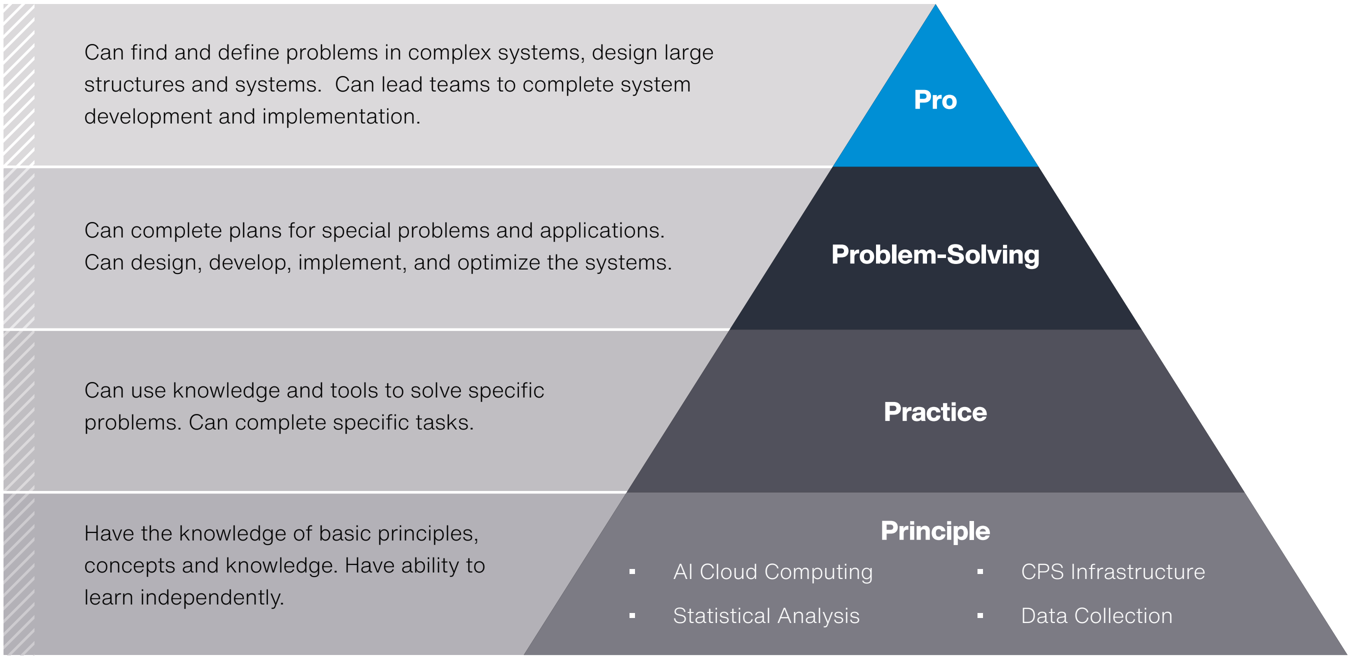

Can find and define problems in complex systems, design large structures and systems. Can lead teams to complete system development and implementation.
Pro
Can complete plans for special problems and applications. Can design, develop, implement, and optimize the systems.
Problem-Solving
Can use knowledge and tools to solve specific problems. Can complete specific tasks.
Practice
Have the knowledge of basic principles, concepts and knowledge. Have ability to learn independently.
Principle
AI Cloud Computing
CPS Infrastructure
Statistical Analysis
Data Collection

Figure 4 - 4P Approach for Industrial AI Talent Development

2.9 CHALLENGES

While the manufacturing sector has made significant strides in integrating AI into its operations, it continues to face substantial challenges. The evolution of sensor technologies, communication protocols, and computing power has dramatically enhanced data and platform technologies, paving the way for the development of advanced analytical tools. As these tools begin to demonstrate their potential, operational technologies are being refined and deployed. Yet, the widespread adoption of Industrial AI in manufacturing is primarily hindered by two factors: the inherent characteristics of manufacturing operations, which rely heavily on large, costly, and often outdated hardware, and the hesitancy of senior management to embrace new technologies in established processes. Additionally, technical hurdles associated with enabling technologies demand attention.

Cybersecurity: It is crucial for safeguarding data integrity, privacy, and confidentiality. Threats can arise at any communication layer or during data transmission, with internet-connected devices often being the initial entry points for cyberattacks. These can include compromised gateways, malware, and cross-site scripting. At the Smart Nodes Layer, integrity attacks aim to corrupt sensor signals or machine control values. Replay attacks, involving repeated retransmission of legitimate data packets, pose a significant risk. The Network Layer is prone to delays in communication, affecting real-time services, with replay attacks being a notable threat here as well. In the Fog Layer, attacks can cause service unresponsiveness or denial, impacting system functionality. High synchronization applications may suffer from de-synchronization due to these attacks. The Cloud Layer, holding valuable data, faces threats like denial of service, data breaches, malware, and unauthorized access. The complexity of these attacks necessitates robust defenses like firewalls and encryption. Blockchain technology offers a promising solution for enhancing security and privacy through decentralization. A unified three-layer architectural proposal aims to tackle these issues effectively.

Data Integrity: The unpredictable nature of manufacturing necessitates rigorous data integrity checks to ensure accuracy, completeness, and bias-free information. This is crucial from data generation to storage, presenting a challenge in large-scale applications where physical validation is impractical.

Data Management: The increasing adoption of AI requires effective management of vast and varied data. Traditional relational databases fall short, prompting exploration of alternatives like NoSQL databases, Hadoop, and Google File System for better scalability and flexibility.

System Availability: Ensuring the reliability of hardware and software is critical, not only for operational continuity but also for maintaining data safety and providing diagnostic information during failures.

Analytics: Transforming data into actionable insights remains a challenge as AI applications expand. Each manufacturing scenario is unique, requiring custom solutions and human oversight for model fine-tuning and validation. The suitability of algorithms varies, and despite computational advances, algorithm performance does not always scale linearly. Real-time data analysis further complicates this, necessitating the development of algorithms that can efficiently process diverse and high-velocity data streams.

Data Quality and Availability: For machine learning and deep learning models to perform accurately, they require large volumes of high-quality, representative data. In many cases, collecting this data is challenging due to privacy concerns, accessibility issues, or the rarity of certain events. Furthermore, the data must be clean and well-labeled, which is a labor-intensive process prone to human error.

Model Interpretability and Explainability: Many machine learning and deep learning models, especially deep neural networks, are often seen as "black boxes" because their decision-making processes are not easily understood by humans. This lack of transparency can be a significant barrier in sectors where trust and understanding the reasoning behind decisions are crucial, such as healthcare and finance.

Conclusion

This chapter delineates the transformative potential of Industrial Artificial Intelligence in smart manufacturing and maintenance, underscoring its distinction from conventional AI. It demonstrates Industrial AI's capacity to enhance operational efficiency, predictive maintenance, and production optimization. The research highlights the necessity of integrating multidimensional learning and domain-specific knowledge, emphasizing the importance of addressing challenges such as cybersecurity, data integrity, and model transparency. In summary, Industrial AI emerges as a pivotal enabler of innovation in smart manufacturing and maintenance, with its success contingent upon collaborative efforts to refine and securely deploy these technologies.

Navigating the Impact of Artificial Intelligence on Labor Dynamics

In today's workforce, AI is a ubiquitous topic, influencing how individuals across all industries perform their daily tasks. With its pervasive impact, most jobs are already feeling its effects, while few remain untouched. However, the transformational potential of AI and the curiosity surrounding its adoption extend far beyond industry boundaries, encompassing diverse cultures and reaching across the globe.

Leadership should embrace a narrative positioning AI as a tool to augment human intelligence. Addressing the human "worries" alongside the manufacturing advancement will bring an organization faster to success and adoption. It's imperative to foster a culture of ongoing AI experimentation to ignite curiosity and foster innovation. By creating room for novel skill development and experimentation, leaders pave the way for a more sustainable and productive future. AI challenges conventional industrial perspectives, offering opportunities to broaden individuals' mindsets and cultivate open-mindedness.

AI brings a new level of transparency to our way of thinking that can also be translated in human relationships. Our approach of taking the framework of AI transformation into human transformation will allow us to create the new jobs of the future with purpose. Just as Industrial AI requires a comprehensive approach, so does human-centric AI. It must be a cross-departmental strategy for leaders at all levels.

AI brings a new level of transparency to our way of thinking that can also be translated in human relationships. Our approach of taking the framework of AI transformation into human transformation will allow us to create the new jobs of the future with purpose.

As we define the meaning of AI and Industrial AI, it is important to recognize the need to define what work means to an employee in a digital environment. The next wave of talent will not require encouragement to use technology, they were born into it. What they need is to see the leaders of today having a strategy focused on how technology benefits their work environment, their careers, and their lives to result in choice and freedom.

Guiding Principles for Integrating Artificial Intelligence

1. AI's Pervasive Impact

AI is a significant concern across industries, transforming most jobs and fostering a global curiosity and eagerness to learn about AI-driven changes.

2. AI as a Collaborative Tool

Emphasizing AI as a complement to human intelligence encourages innovation, creativity, and open-mindedness, leading to a more sustainable and productive future.

3. Human-Centric AI Strategy

Successful AI implementation requires a comprehensive strategy involving all leaders, focusing on understanding and addressing both visible and invisible workforce challenges, such as employee engagement and adaptability.

4. Workforce Engagement and Connection

Defining the meaning of work in a digital environment is crucial. Strategies should prioritize connection and meaningful engagement, leveraging AI to empower teams and maintain a sense of purpose.

5. Technology Integration for the New Workforce

The technologically native workforce needs leaders to demonstrate how AI and digital tools enhance their work environment, careers, and personal lives, promoting a sense of choice and freedom.

Key Action Items

01

Adopt Comprehensive Industrial AI Solutions

Move beyond traditional AI applications and embrace Industrial AI to address both visible and invisible challenges in manufacturing. Implement predictive analytics and intelligent management tools to enhance productivity, quality, and operational efficiency.

02

Invest in Expertise and Collaboration

Foster collaboration between computer scientists, AI experts, and domain-specific professionals to develop tailored Industrial AI solutions. Invest in training and upskilling your workforce to leverage the full potential of Industrial AI technologies.

03

Enhance Regulatory Frameworks

Develop and implement policies that promote the responsible use of Industrial AI. Ensure that regulatory frameworks keep pace with technological advancements, addressing issues related to data privacy, security, and ethical considerations in AI applications.

03

Cybersecurity Resilience for Advanced Manufacturing

Mike Wilkes

Adjunct Professor
Department of Technology Management & Innovation
New York University

Jim Davis

Faculty Advisor Office of Research
Principal Investigator CESMII

NYU

UCLA Advanced Research Computing

3.1 INTRODUCTION

The intersection of data management and cybersecurity is critical to the success of advanced manufacturing and national security. This chapter aims to examine best practices and provide a way to safeguard industry as it evolves through technological trends. The narrative weaves together threads of resilience, transformation, and adaptation, demonstrated through compelling case studies. From the remarkable strides in AI-driven material discovery within autonomous labs to groundbreaking advancements in tissue fabrication techniques, these examples serve as poignant reminders of the profound shifts reshaping the manufacturing landscape.

However, the scope goes beyond cybersecurity and into the world of global security as well. As we peer into the future, the trajectory of our digital economy hinges upon our collective ability to embed sustainable practices within the fabric of Industry 4.0. In this epoch of unprecedented technological velocity, cybersecurity resilience emerges not just as a requisite for industry advancement, but as a cornerstone of national security itself.

3.2 EXECUTIVE SUMMARY

The U.S. National Strategy for Advanced Manufacturing has prioritized clean and sustainable manufacturing, microelectronics, bioeconomy, new materials, smart manufacturing, talent, supply chains and advanced manufacturing ecosystems. These priorities all converge on and foundationally depend on data-centered interconnectedness, integration, interoperability, and innovation at scale. Cybersecurity and addressing unwanted intrusions of manufacturing data become intertwined with trusted and scaled use of data for desired sharing and exchange of data. The current state of US advanced manufacturing is presented through the lens of cybersecurity best practices. From this basis of analysis, the authors identify and focus on emerging trends that present a set of challenges and opportunities for the industry as it seeks to modernize and transform itself into what has been termed "Industry 4.0" or the Fourth Industrial Revolution. A focus is placed on sustainable approaches to determine whether our digital economy evolves or stagnates.

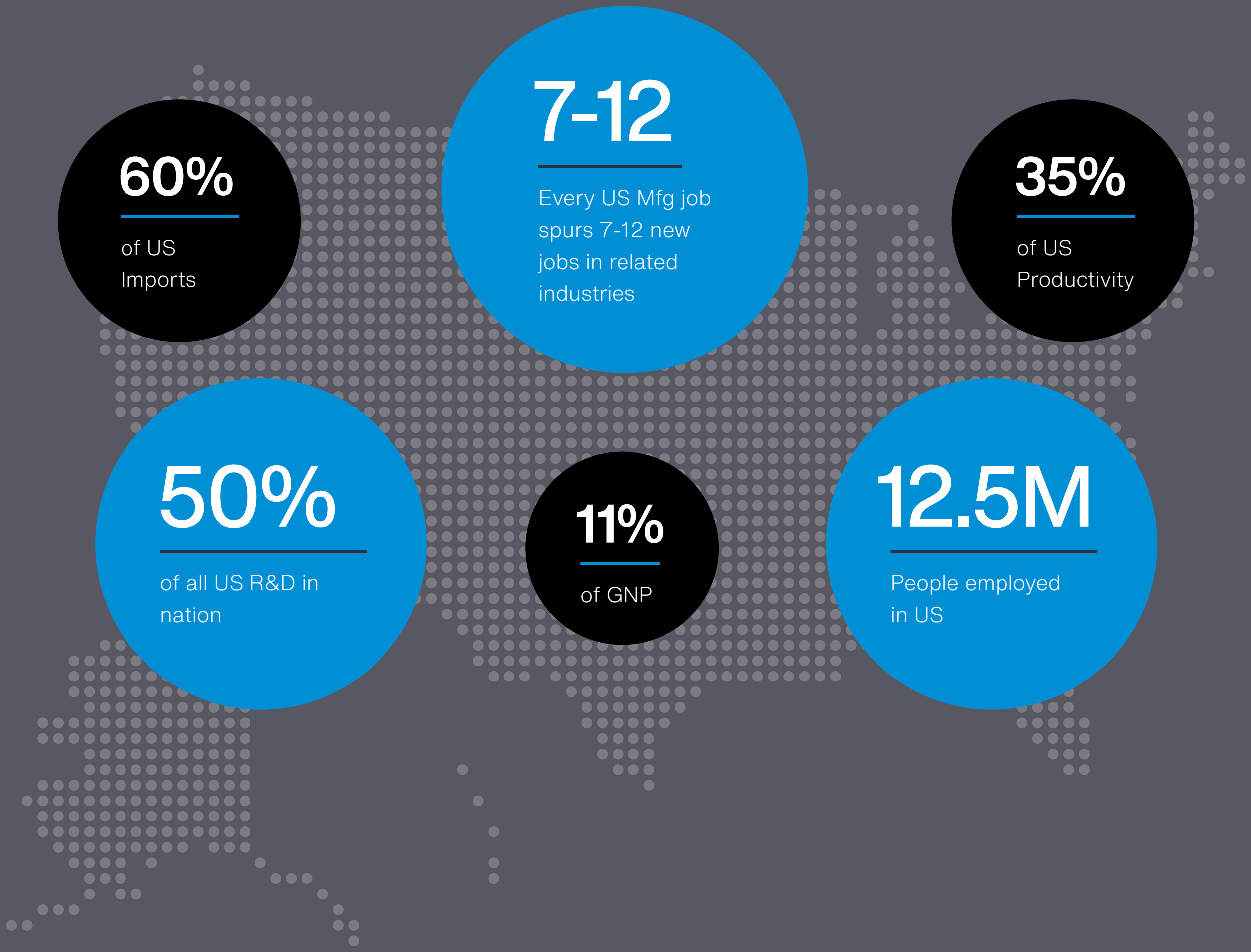
The giddy enthusiasm for the "pure possibility" of certain aspects of this transformation is balanced with pragmatic realities of a world in which (1) data and IT security are vital to ensure physical operations are conducted to expectation, (2) managing IP and trade secrets with trust are vital to economic viability in a global market structure, (3) social, environmental and economic pressures are increasing, and (4) the recognition that there are geopolitical constraints on how this technological shift combining the physical, digital, and biological worlds of manufacturing play out.

Identifying the core drivers of innovation and opportunity are key to creating an understanding of possible futures and paths towards what might seem like science fiction just a few decades ago. Whether we find ourselves living in a utopian or dystopian society depends upon whether we manage to incorporate sustainable approaches to securing and protecting these new engines of production.

The analysis is peppered with several case studies and references that illustrate the main themes of resilience, transformation, and adaptation. Whether that is peeking inside of autonomous labs where AI is hard at work rapidly discovering novel materials and successfully synthesizing those new compounds or marveling at new tissue fabrication techniques using "acoustic tweezers" to assemble stem cells in densely packed three-dimensional lattices mimicking actual human cardiovascular structures.

Today's simple 3D printers performing extruded plastics are merely crude prototypes of what will, with the continued advancements of nanotechnology and atomic-scale robotics, eventually deliver the Star Trek replicator. Such leaps and bounds that accompany these advances in technology are often quite indistinguishable from magic. Just as the shaman and soothsayer transformed from their pursuits of alchemy and ritualistic sacrifice into the Royal Society with the advent of the scientific method and new tools of inspection of how the world works, so surely will our current understandings of quantum entanglement and time-space be seen as crude approximations of greater truths and knowledge by those who come after us.

WHY IS SUPPORTING US MANUFACTURING IMPORTANT?



60%
of US Imports

7-12
Every US Mfg job spurs 7-12 new jobs in related industries

35%
of US Productivity

50%
of all US R&D in nation

11%
of GNP

12.5M
People employed in US

Source - National Association of Manufacturers

3.3 AN OVERVIEW OF CYBERSECURITY, DATA MANAGEMENT AND US ADVANCED MANUFACTURING

The US advanced manufacturing industry is experiencing a multitude of changes in response to several key shaping forces. These forces include new and emerging technologies and trends, such as artificial intelligence, machine learning, robotics process automation, code manufacturing, integrated workflows, real-time supply chain processes, and ubiquitous data pipelines. Clear implications and imperatives exist within the industry around both challenges and opportunities, but the overarching factor affecting change in manufacturing is not the advanced technologies themselves but rather customer expectations.

Advanced technologies are an accelerant to the process of change and the evolution of manufacturing, but they do not exhibit the directional influence the way customer experience currently drives industry outcomes. Advanced technologies offer ways to better use resources, prevent and address unwanted outcomes, and make materials that are better for the world. Advanced manufacturing, however, responds best to demand. Together, advanced manufacturing and advanced technologies combine to create the ability to reveal the impacts of that demand to influence customer, industry, and government decisions and enable new economies to drive product innovation.

On Technology

When someone speaks about technology, information security or cybersecurity in 2024 there is a very high probability that they are referring to electronic circuits, networking protocols and a vast array of digital technologies. But it is important to point out the meaning of the word technology in a more general sense. Strictly speaking, technology is not just the domain of bits and bytes. Any system of information, including a 1934 multi-volume, leather-bound encyclopedia set or an ancient Mesopotamian vault full of cuneiform clay tablets ought to be included in our definition of information system.

Technology =

techne meaning

“art, skill, cunning of hand”

+

logia meaning

“a subject or study of interest”

Embracing this larger definition of technology allows us to include many more systems than those defined by computer processors manipulating ones and zeros. Information systems and the data they contain have evolved over time and will continue to evolve in the future. We are seeing that evolution firsthand and up close.

The Data

Before we can talk about how to protect the data and intellectual property of advanced manufacturing, we need to first talk about the data itself. Information security has three foundational pillars: confidentiality, integrity, and availability. Before we think about how much security to put around an information system or an application or service, we need to classify the data that the system or application contains. Information security begins with data classification and is typically grouped into a minimum of four categories:

- Public
- Internal
- Confidential Sensitive
- Confidential Restricted

Keep in mind that data classification is not always a static thing. Data classifications can be dynamic and can change over time. In such situations it is not "set and forget." Some kinds of data move or transition, for example, from Confidential Restricted into Public such as Marvel movie casting decisions or Supreme Court opinions. Leading up to the moment of publication and sharing of this information, the data classification is extremely sensitive. This is also the case with earnings call data published by publicly traded companies. This means that some systems will need to adopt what is termed a "bitemporal" database structure for the data that it contains. The interface to the data needs to be able to support queries about the data classification for a record or dataset of records "as of a particular date."

Information security has three foundational pillars: confidentiality, integrity, and availability.

Metadata

On-prem and cloud-based data storage solutions can label or tag the storage buckets, blobs, folders, and file systems used in business processes. This is known as "metadata" and is essential to our ability to keep abreast of the demands of growth. Modern best practices for data management include always having this "metadata" available to facilitate, among other reasons, data audits where the provenance and lineage of data are important elements. More on these terms a bit later. Good data management and data classification should strive to be automated and repeatable to avoid human error and in order to scale. According to Statista, global data creation will increase to more than 180 zettabytes by 2025, which is about 50% more than in 2023. Put another way, this is more than 300 million petabytes being created per day in 2024.

180
zettabytes

300m
petabytes

Global data creation will increase to more than 180 zettabytes by 2025, which is about 50% more than in 2023. Put another way, this is more than 300 million petabytes being created per day in 2024.

To achieve this "effortless audit" capability of metadata, devops, SRE and data engineering teams should make sure to populate at least four tags or labels of name-value pairs:

Name	Example Values	Notes
Owner	Named individual (ssmith) or team (devops)	Data discovery and automated classification is enabled by having owners assigned to data.
Environment	prod, qa, dev, test, admin	Audits and reviews are more easily scoped when the environment tag/label is populated with info.
Data_Classification	public, internal, confidential sensitive, confidential restricted	These are just four of the more common data classifications. If mixed data is present, the highest classification should be applied.
Data_TTL	7d, 180d, 3y, 7y, 30y	For how long should the data classification be maintained?

Because of the primacy of data in the modern digital economy we have terms such as data catalog, data dictionary, data discovery and data mapping. For quantum security reasons, while we are required to build a data catalog and data mappings for GDPR (General Data Protection Regulation) compliance around PII (Personally Identifiable Information) we should also be thinking about the TTL (Time-To-Live) for the confidentiality of data. How long does this data need to remain secret? Your DNA, probably a long time. Your bank account password, maybe a week. If we rotate our bank account passwords every seven hours using a password manager, then we can mitigate the risk of a CRQC (Cryptographically Relevant Quantum Computer) being used to attack and decrypt our bank account login within eight hours.

Existing data management practices within manufacturing processes fall into four areas: data storage, data transmission, data access protocols and data provenance.

Data Storage

Manufacturing processes typically involve the generation of large volumes of data, ranging from product specifications and quality control metrics to equipment performance and maintenance records. These data will exist as many different types. The data that are most valuable have been collected, ingested and contextualized with respect to namespace, units, and use with a machine or operation. To be of full use, data will have also been selected, categorized, engineered and aggregated for in-process context and solution objectives.

The current trend is towards utilizing cloud-based storage solutions, which offer scalability, accessibility, and the ability to store diverse data types. Cloud storage enables manufacturers to centralize their data, facilitating real-time collaboration and analysis. However, concerns regarding data security and potential latency issues may arise, especially in scenarios where a reliable internet connection is not guaranteed.

On-prem storage solutions are still prevalent, providing a sense of control and security over sensitive data. However, these solutions may face challenges in terms of scalability and the cost associated with maintaining hardware infrastructure. Advanced manufacturing is further increasing demand for inter-factory, inter-company, supply chain, and ecosystem data exchange that change long-held views on security and this kind of industry scalability.

> **Advanced manufacturing is further increasing demand for inter-factory, inter-company, supply chain, and ecosystem data exchange that change long-held views on security and this kind of industry scalability.**

Data Transmission

The effectiveness of data transmission protocols is crucial for ensuring the seamless flow of information across different stages of the manufacturing process. Many manufacturing facilities have adopted Industrial Internet of Things (IIoT) devices and sensors that generate real-time data. The use of standard communication protocols such as MQTT or OPC UA has become common to facilitate the exchange of data between devices and systems. However, ensuring the reliability and security of data transmission remains a priority.

Challenges may arise in environments with legacy systems that may not be compatible with modern communication protocols. Additionally, concerns about data integrity and potential cyber threats highlight the need for robust encryption and authentication measures.

Data Access Protocols

Efficient data access is crucial for decision-making in manufacturing processes. Manufacturers often implement Manufacturing Execution Systems (MES) or similar platforms to monitor and control production activities. These systems provide a centralized interface for accessing real-time data, enabling operators and managers to make informed decisions.

Integration with data analytics tools and business intelligence platforms enhances the ability to derive meaningful insights from the collected data. However, challenges may arise in ensuring that relevant personnel have timely access to the data they need, and issues such as data silos or lack of interoperability between different systems can hinder the overall effectiveness of data access protocols which in turn limit the value of the data in a broadening advanced manufacturing context.

Data Provenance

Understanding and maintaining data provenance is gaining increasing importance. Data provenance refers to the origin, lineage, and history of data, including information about its creation, modification, and movement throughout the manufacturing process. It plays a critical role in ensuring the integrity, trustworthiness, and compliance of the data.

Manufacturers are becoming more conscious of the need to trace the entire lifecycle of data, especially in regulated industries where compliance with standards and regulations is paramount. Knowing the origin of data is crucial for quality control, auditing, and addressing issues such as product defects or recalls. It is also essential for broadening the use of data with trust, i.e. aggregating data to build more robust data sets or exchanging data for operational interoperability.

Effective data provenance practices involve implementing mechanisms to capture and store metadata, timestamps, and other relevant information associated with each piece of data.

Effective data provenance practices involve implementing mechanisms to capture and store metadata, timestamps, and other relevant information associated with each piece of data. Blockchain technology, for instance, is being explored to create immutable and transparent records of data provenance, providing a decentralized and secure way to track the history of data changes.

Challenges in data provenance include the complexity of modern manufacturing ecosystems, where data may be generated by various devices, sensors, and systems. Ensuring a standardized approach to capture and manage provenance across different data sources remains an ongoing concern. As technology continues to evolve, integrating robust data provenance practices will become a key aspect of comprehensive data management strategies in manufacturing.

In conclusion, while modern manufacturing processes have embraced advanced data management practices, challenges still exist. Striking a balance between centralized cloud storage and on-prem solutions, ensuring the reliability of data transmission protocols, and addressing access challenges are essential for maximizing the effectiveness of data management in manufacturing. Ongoing advancements in technology and industry standards will likely shape the future landscape of data management within the manufacturing sector.

How to Protect the Data

Once we have tagged and classified our data and understand which data is most sensitive to disclosure and unauthorized access, we are then faced with the challenge of protecting that data. This can seem a daunting task given the fact that data is like water flowing downhill. It will always find a way to reach the bottom of the hill despite our efforts to contain and direct its flow. Therefore, it is sometimes the case that cyber security controls and procedures are the very thing that gives rise to "workarounds" by users to get data where it is needed, often side-stepping the security controls that have been created to protect that data. Cybersecurity professionals need to keep this point in mind: for every security action, there is an equal and opposite user reaction.

Just as Newton's Third Law of Motion states that for every action, there is an equal and opposite reaction, the same principle applies in the realm of cybersecurity.

Security Action: Require strong passwords
User Reaction: Write it on a Post-it® note

That said, there are some novel techniques and technologies that can be applied to solving this problem and the dynamic described above because data often becomes more valuable when it is shared. Three protection approaches to consider are: data masking, data object encoding and data minimization.

Data Masking

In the realm of data security, one crucial technique that plays a pivotal role in safeguarding sensitive information is data masking. It is imperative to underscore the significance of this technique in protecting data from disclosure and breach. Data masking, also known as data obfuscation or data anonymization, involves the transformation of confidential information into a fictional but structurally similar version, rendering it unreadable and irrelevant to unauthorized users. This process ensures that sensitive data remains concealed, even if accessed by individuals without proper authorization.

The primary objective of data masking is to strike a balance between data usability and security. By adopting various masking methods such as substitution, shuffling, and encryption, organizations can mitigate the risk of unauthorized access while still enabling the utilization of masked data for development, testing, or analytical purposes in non-production environments. The process of taking production data into a "lower" environment for testing is known as a "downwards refresh" and the security of such a workflow is greatly improved by data masking as this happens. It is crucial for data engineering teams to comprehend the intricacies of data masking techniques, as they are fundamental in maintaining compliance with data protection regulations and fortifying the overall security posture of an organization. Through research and with the careful application of machine learning and generative AI we can employ data masking as a core data security practice, ensuring the confidentiality and integrity of sensitive information in an increasingly interconnected world.

Data Object Encoding

Data Object Encoding, particularly in the context of Trusted Data Format (TDF) as defined by the Office of the Director of National Intelligence (ODNI), is a crucial technique employed for secure and standardized representation of information. TDF serves as a framework for encoding and structuring data to ensure trustworthiness, integrity, and confidentiality. This technique involves the transformation of data objects into a format that is not only machine-readable but also adheres to stringent security standards. TDF facilitates interoperability among diverse systems and applications, allowing for seamless data exchange within trusted environments. By employing advanced encoding methods, TDF ensures that sensitive information remains protected from unauthorized access or tampering. This approach plays a pivotal role in fostering information sharing and collaboration across intelligence and security domains while maintaining the highest levels of data security and reliability.

One of the notable features of TDF is the ability to have data policy that follows the data as it leaves a network and to be able to enforce that policy remotely. An example of the utility of TDF is to have a business document with an appendix which is redacted for specific domains or users and readable for others that are defined as approved. The phrase "locking the barn door after the horses have left" used to be applicable to data exiting your organization, but now thanks to the intelligence community research and development, we have new options for protecting that data. The TDF is freely available with no restrictions and requires no use of proprietary or patented technology and is thus open for anyone to use.

Data Minimization

Data minimization is a strategic technique employed in information security to safeguard sensitive data from unauthorized disclosure and access. The principle behind data minimization is to collect, process, and retain only the minimum amount of data necessary for a specific purpose. By limiting the scope of stored information to what is essential, organizations can significantly reduce the potential impact of a data breach or unauthorized access. This approach not only mitigates the risks associated with data exposure but also aligns with privacy principles, ensuring that personal and sensitive information is handled responsibly. Data minimization helps organizations streamline their data storage practices, making it more manageable to implement robust security measures and maintain compliance with privacy regulations. By embracing the concept of data minimization, entities can enhance their overall cybersecurity posture and foster a privacy-centric approach to data handling and protection.

The primary objective of data masking is to strike a balance between data usability and security.

Data
Usability
Security

3.4 EMERGING TRENDS

In the dynamic landscape of the advanced manufacturing industry, data security has become a paramount concern, steering the industry towards innovative solutions to safeguard sensitive information. The advent of smart manufacturing, characterized by the integration of cutting-edge technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI), has ushered in a new era of efficiency and connectivity. Concurrently, the rise of digital twins, virtual replicas of physical systems or processes, has provided unprecedented insights and optimization capabilities. However, as the industry increasingly relies on interconnected digital ecosystems, the specter of data breaches looms large. In this milieu, staying ahead of emerging trends in data security has become imperative for manufacturers seeking to harness the full potential of advanced technologies while fortifying their defenses against potential cyber threats.

Smart Manufacturing

We are clearly begging the question when putting the word “smart” in front of anything. Smart TVs, smart phones, smart food, or smart cities. Previous TVs, phones, food, and cities were not technically “dumb” of course, but there is a common thread to using the phrase “smart manufacturing” and the intention of those using it. We are essentially talking about using connected technologies to deliver new possibilities to the production process. The term was coined in 2007, the year Steve Jobs introduced the world to the first iPhone.

CESMII (Clean Energy Smart Manufacturing Innovation Institute) is a Manufacturing USA Institute sponsored by the Department of Energy. CESMII’s program home and headquarters is with UCLA. As defined by CESMII, Smart Manufacturing (SM) is the digital transformation of the manufacturing industry for proactive management and automation of assets, line and factory operations, supply chains and ecosystems. SM both enables and derives maximum value with scaled industry adoption, increased productivity, precision and performance at all levels of manufacturing. The ability to execute on industry-wide strategies requires investment in people, technology, and practice that enables manufacturers to extract

Smart Manufacturing is at the Heart of Industry 4.0 and the Promise of:

- Improved Data Insights
- Maximized Plant Efficiency
- Maximized Plant Efficiency
- Faster Issue Resolution
- Tracking Products Across Value Chain
- Seamless Data Exchange
- Better Safety and Quality Control
- Continual Production Improvement
- Ensure On-Time Delivery
- Supply Chain Resilience

significantly increased value from existing assets and resources operating at network scale. It also requires digitalization to empower more effective workers, factories and supply chains. SM broadens understanding of the manufacturing process through real-time data and the ability to make information-driven, proactive decisions to improve operational efficiency, quality and energy productivity.

SM is enabled by the scaled integration of networked data for plantwide optimization, sustainable production and resilient, demand driven supply chains. Integration is internally focused within every factory and externally extended throughout all inter-factory operations, supply chains and resource ecosystems. SM has a line of sight to an industry that is networked with secure and trusted data interconnectedness at every level from sensor, to machine or device, to operation, line operation, factory, inter-factory, supply chain and ecosystem.

CESMII has worked with almost every industry segment to demonstrate and champion the significant economic and environmental benefits of SM at both factory and supply chain levels. These demonstrations encompass factory and supply chain, raw material-to-product use, productivity, precision and performance. In existing industries, there is significant economic gain; energy and material consumption are reduced, greenhouse gas emissions are reduced and there are step change improvements in environmental health, safety and product traceability. Maintenance costs drop dramatically, operational uptime is increased, and operations can be optimized to higher-level, multi-objective key performance indicators including shared supply chain models and overall end-to-end visibility.

From a business standpoint, Smart Manufacturing both pulls and pushes on new business models to drive competitiveness and extract the full value of newly created data. Proactive management, end-to-end productivity, product lifecycle, and new economies with new businesses and new factory locations have re-defined “resilience.” Small, medium, and large manufacturers can all integrate into supply chain and industry sustainability strategies. Data-driven automation and autonomy address increased complexity while augmenting the essential roles of people. With the adoption of SM there is faster development and assimilation of new materials and new physical technologies. SM enables global ESG (Environmental, Social and Governance) priorities incorporating carbon accounting, climate leadership plus transitioning to circular economies, low carbon fuels, electrification and new clean energy technologies.

Digital Twinning

In the ever-evolving landscape of manufacturing digitization, the integration of digital twins has emerged as a crucial element in fortifying information security protocols. As noted with Smart Manufacturing above, digital twins are the front-facing cyber applications that, when developed and synchronized with data, produce scaled productivity, performance, and precision gains. Digital twins in this sense encompass cyber system models of manufacturing operations, products, and materials from sensors to supply chains and span a full range of mathematical, AI/ML, physics-based, physics-informed and high fidelity modeling methods. As such these models not only describe, predict, and prescribe views of the physical operations but they also offer means of understanding expectations with which to address cybersecurity.

> **As an active practitioner of information security and as instructors in higher education, we are deeply engaged in exploring the intersections of technology and industry, highlighting the significance of employing digital twins to enhance cybersecurity in manufacturing processes.**

As an active practitioner of information security and as instructors in higher education, we are deeply engaged in exploring the intersections of technology and industry, highlighting the significance of employing digital twins to enhance cybersecurity in manufacturing processes. These virtual replicas of physical systems offer a real-time, dynamic representation of the production environment, allowing for comprehensive monitoring and analysis. By leveraging digital twins, manufacturers can identify vulnerabilities, assess potential threats, and simulate security scenarios to proactively strengthen their defenses. Furthermore, the integration of advanced analytics and artificial intelligence within digital twins provides the ability to detect anomalies and predict potential security breaches, enabling a proactive approach to safeguarding sensitive data and critical infrastructures. The advent of Smart Manufacturing and digitalization when integrated with strong security offers significant new capabilities to address operational resilience. However, if digitalization and security are not integrated the industry will actually increase its security exposure and decrease its ability to mitigate threats and intrusions.

In our research, lectures, and conference presentations, we emphasize that the adoption of digital twins in information security protocols not only enhances the resilience of manufacturing systems but also facilitates adaptive responses to emerging cyber threats. The ability to simulate and test security measures within the virtual realm enables manufacturers to refine and optimize their defenses before implementation in the physical environment. As we navigate the era of Industry 4.0, it is imperative for asset owners and operators alike to comprehend the pivotal role that digital twins play in establishing robust cybersecurity frameworks. Digital twins are as much about the data on which they depend as the model configuration itself. By staying at the forefront of technological advancements and embracing digital twinning technologies, the manufacturing sector can more effectively mitigate risks, ensuring the integrity, confidentiality, and availability of critical information in an increasingly interconnected digital landscape.

Zero Knowledge Database

The concept of a Zero Knowledge Database (ZKDB) emerges as a formidable technique for safeguarding sensitive data within the advanced manufacturing sector. In an era where data integrity and security are paramount, ZKDB provides an innovative solution by allowing queries to be performed on the database without revealing the underlying information. This cryptographic protocol ensures that only the necessary results are disclosed, eliminating the need for exposing raw data. In the advanced manufacturing landscape, where proprietary designs, production processes, and intellectual property are at the core of competitive advantage, ZKDB acts as a robust shield against unauthorized access or data breaches. By maintaining a zero-knowledge proof system, manufacturers can confidently collaborate, share, and analyze critical information without compromising the confidentiality of their proprietary data, thereby fostering a secure and collaborative environment within the industry.

> **By maintaining a zero-knowledge proof system, manufacturers can confidently collaborate, share, and analyze critical information without compromising the confidentiality of their proprietary data...**

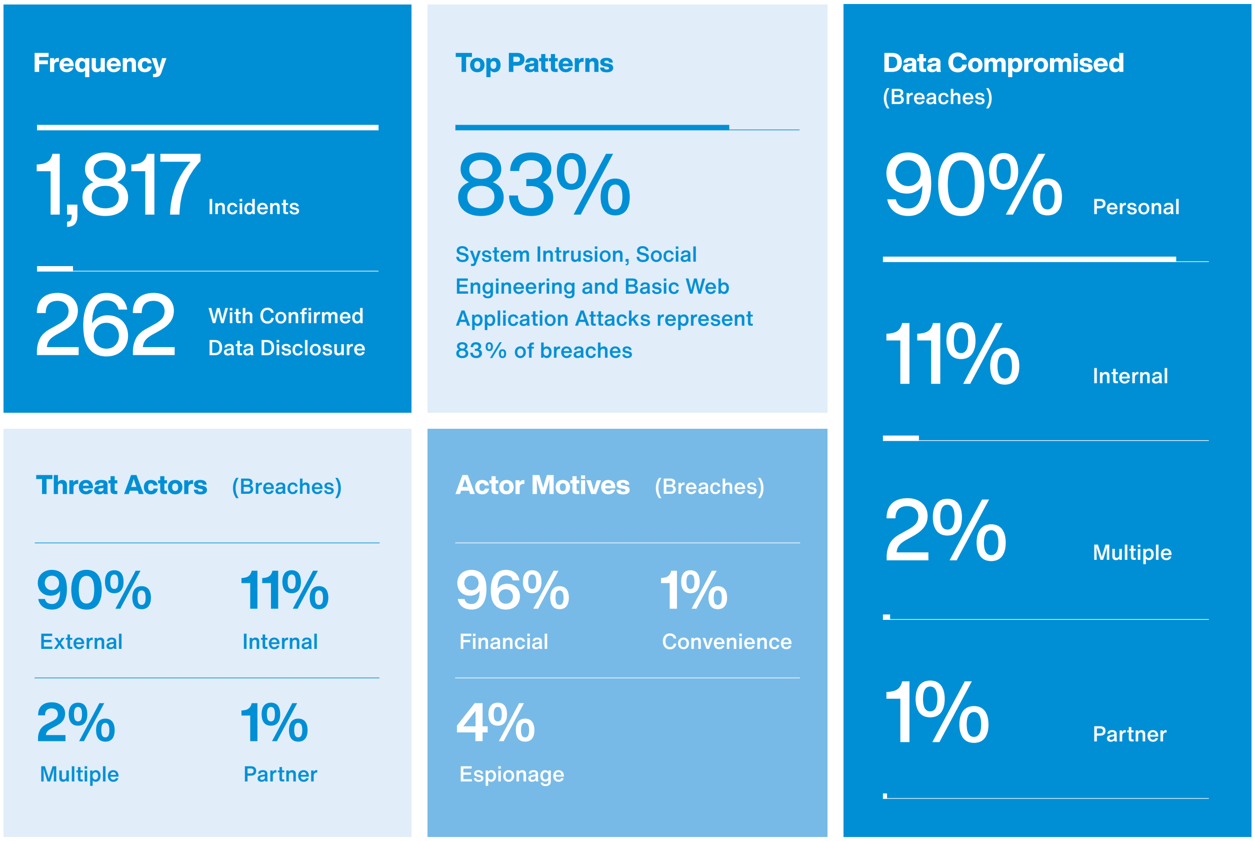
Breaches, Leaks and Data Spillage

Breaches, leaks, and data spillage refer to incidents where sensitive, confidential, or protected information is exposed to unauthorized individuals or entities, posing significant security and privacy risks. These events can result from cyberattacks, human error, or system vulnerabilities, often leading to severe financial, reputational, and legal consequences for affected organizations.

Breaches are not the only kind of service disruption that US Advanced Manufacturing needs to contend with and to address. DoS (Denial of Service) attacks and DDoS (Distributed Denial of Service) attacks accounted for approximately 67% of incidents in the manufacturing sector according to the Verizon DBIR. Compromised computers and other internet-connected "smart devices" usually running an embedded version of the Linux operating system are orchestrated to launch massive attacks against a company's infrastructure. Mitigating these attacks involves deploying robust network security measures, such as traffic filtering, load balancing, and the use of anti-DDoS services, to detect and block malicious traffic while ensuring legitimate user access remains available. Google, for example, mitigated an attack that peaked at 398 million requests per second (RPS), more than eight times larger than the previous record. This August 2023 attack targeted Google Cloud infrastructure, Google services, and Google's customers.

MANUFACTURING INDUSTRY DATA BREACH

Verizon 2023 DBIR (Data Breach Investigations Report)



Frequency

1,817 Incidents

262 With Confirmed Data Disclosure

Top Patterns

83%

System Intrusion, Social Engineering and Basic Web Application Attacks represent 83% of breaches

Data Compromised (Breaches)

90% Personal

11% Internal

2% Multiple

1% Partner

Threat Actors (Breaches)

90% External

11% Internal

2% Multiple

1% Partner

Actor Motives (Breaches)

96% Financial

1% Convenience

4% Espionage

3.5 CHALLENGES AND OPPORTUNITIES

Given the frequency of attacks and disruptions that we can expect heading into the next few years of increasing digitalization of manufacturing, one of the biggest challenges is also one of the biggest opportunities: risk assessments. The industry is not without several frameworks and compliance standards that can be used to measure and prioritize gaps in cybersecurity programs operated by (according to IBIS World) the 623,066 manufacturing businesses in the US as of 2023. Having an independent third party conduct a risk assessment of a business annually is a recognized best practice. But what percent of those 600k+ manufacturing businesses have taken that proactive risk management step in the last year?

623,066

Manufacturing businesses in the US as of 2023

70%+

More than 70% of companies investing in advanced analytics, AI, or 3D printing fail to move beyond the pilot phase

Whether a company selects NIST CSF v2.0, CIS Top Controls v8, TISAX version 6 or ISO 27001:2022 for their compliance audit and risk assessment depends on industry, geography and business size. There is no reason, however, for each and every one of these businesses, whether mandated by a regulatory agency for their industry or not, to step into an improved state of awareness of their risks by performing an assessment. And of course awareness of exposure to risk is not sufficient as we must then take action to eliminate or mitigate the gaps. In fact, it is also very likely the case that your IT department has been asking for the resources to address items in the corporate risk register but have not been supported with the requisite people, process or tools to confront the sources of risk. Practical mitigations are available and not every major risk requires spending millions of dollars in software or hardware. Reach out and engage a trusted cybersecurity advisory firm and start building a plan around your exposed assets.

The global manufacturing industry has been lagging in the adoption of advanced technologies. More than 70% of companies investing in advanced analytics, AI, or 3D printing fail to move beyond the pilot phase of development because advanced manufacturing requires factories to think through and establish the necessary investments in data and modeling infrastructure, tools, methods and governance that are required. Those that do manage to adopt advanced technologies are positioned to stride with confidence into the future of electric vehicles, AI-driven discovery of novel compounds, aerospace engineering, medical sector advances in tissue fabrication and nano-scale assembly of products and much more.

> As managers we execute a plan,
> as leaders we manage scarcity, and
> as executives we manage ambiguity.

Greg Wood

Former SVP of Technology Risk Management and
Security at The Walt Disney Company

Asset Ownership

When thinking about asset ownership we are clearly in the domain of public-private partnerships because 85% of critical infrastructure assets are owned by the private sector. Public/private partnership is not a nice to have, but a requirement. So, while historically the relationship between private sector operations and public sector oversight has been categorized as more of a challenge, we are seeing signs that an improved relationship is emerging. The government is investing in national institutes and regional hubs that can support and facilitate intra- and inter-company capabilities as well as new vendor-manufacturer data relationships. With respect to security, a one-way sharing of information from the private sector to the government is not really a partnership. It feels more like "reporting," but two-way sharing of information through the MFG-ISAC founded in March of 2022, for example, becomes a valuable partnership with and among the government and asset owners.

> **Public/private partnership is not a nice to have, but a requirement.**

Drivers of Innovation

Several factors contribute to the advancement of manufacturing in the United States and other developed nations. One overarching factor is the integration and adoption of advanced technologies that foundationally depend on data and more specifically, depend on contextualized data that remains usable across multiple applications. The use of cutting-edge technologies such as automation, artificial intelligence, robotics, and the Internet of Things (IoT) is having a profound impact on the manufacturing sector. It is not a stretch to characterize the energy and enthusiasm for the transformative aspects of advanced technologies as contributing to a "giddy" sense of opportunity and excitement for the possibilities of improved efficiency, environment sustainability and increased quality of production. Here are some key aspects and their historical precursors:

Automation and Robotics

The use of automated systems and robotics in manufacturing processes enhances efficiency, precision, and productivity. Automation reduces labor costs and accelerates production cycles, leading to improved overall competitiveness.

We must remember that Industry 1.0 thought that it was delivering transformative power to cottage industry and craftsman skills of production using human labor. Steam power and machines characterized this revolution of the 18th century and indeed it was deeply transformative to society.

Continuing this through line we see electricity make its mark in the 19th century with the birth of the "electric grid" lighting up the New York offices of JP Morgan with Thomas Edison's direct current power lines and generators. And after a period known as the "current wars," we see

Nikola Tesla's alternating current emerge as the de facto standard for long distance transmission and distribution of electricity (though it was only in November of 2007 that Con Edison stopped delivering DC current to its final customer in midtown).

Artificial Intelligence (AI)

AI applications, including machine learning and predictive analytics, play a crucial role in optimizing production processes, quality control, and supply chain management. AI enables manufacturers to make data-driven decisions, identify patterns, and enhance operational efficiency. Scaling Smart Manufacturing, with its foundations in data-centered modeling and AI, has been spurred by the promise of predictive modeling, the resurgence in AI and the potential for digital twins. Interconnectedness with meaningful data, applications and tools have become a priority for spanning operations, factories, supply chains, and ecosystems.

The full value of AI in smart manufacturing will require new business models centered around the value of data and how it is secured and protected and the recognition that we derive powerful insights from the network effects of gathering data at scale. Cooperative engagement on AI/ML for operational productivity is a pathway to learn, scale and draw value from data accumulated from years of experience on common problems; derive new insights on factory operations and products; lower many of the costs of entry; and attract more investment on industry specific challenges. The line of sight to interconnectedness, network effects, and a manufacturing web is documented in the NIST Report Towards Resilient Manufacturing Ecosystems Through Artificial Intelligence – Symposium Report.

What becomes important is that AI/ML using operational data depends upon and draws value from business data and market data. In manufacturing there is a wealth of data which embeds years of operational experience but these data are historically siloed. More importantly, operational data are associative. As powerful as AI/ML is, it can only offer reflections on the data to which it has been exposed and that data is (by definition) retrospective. This means that AI systems which are constructed from and trained on limited data are necessarily limited in value. However, the ability to scale and aggregate data offers a far richer data volume of associations for building more robust algorithms. When data are aggregated, there is a far richer set of associations and far greater probability that there is a valuable association. First principles, physics-based digital twins (i.e. machines and process operations) offer directionally predictive capabilities, but are generally insufficient in compensating for the richness of data. By developing machine learning-based digital twins together with physics-based digital twins, both improve each other's fidelity. Cost and time-to-benefit will drive which approach leads to more immediate benefit.

Covered much more extensively in another chapter of this book on the role of AI in the transformation of manufacturing, we would be remiss if we did not mention the sudden maturation of LLMs (Large Language Models) in the fall of 2022 by the popularization of and widespread access to ChatGPT and its variants.

The swift and complete fascination of business and government and academia with prompts and prompt engineering has been nothing short of ubiquitous. It remains to be seen, however, given some of the legal cases that will set the precedent for whether such tools are truly transformative or just copyright infringement “as a service” and a super-hyped solution in search of a problem to solve.

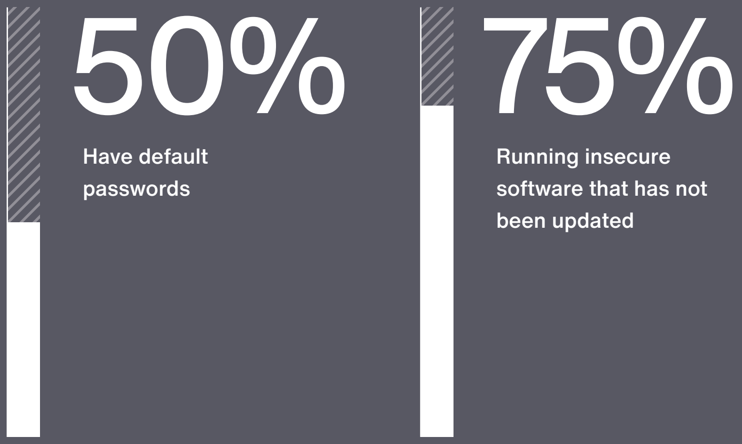
Internet of Things (IoT)

IoT connects physical devices and sensors to the internet, facilitating data exchange and real-time monitoring. In manufacturing, IoT enables predictive maintenance, remote monitoring, and the creation of smart factories that can adapt to changing conditions.

From a cybersecurity perspective, this trend lives up to the hype and attention-getting impacts for risk to society and our digital economy. Putting an IP address on sensors, cameras, sidewalks, streetlights, rock crushers, cars, drones, smart greeting cards, cows and satellites requires a bit of level setting.

If we imagine that there are roughly 10 million interesting computers in data centers across the globe, most of them live in a data center in the U.S. Estimating the number of laptops and mobile devices at around 5 billion, we can see that these devices are more equitably distributed among Earth’s population of just over 8 billion. But looking at IoT devices we are talking something on the order of 50 billion (and growing

Now consider that 50% of these IoT devices have default passwords and that 75% of them are running insecure software that has not been updated (and in many cases, cannot be updated) and we have a big big problem.



of course). Now consider that 50% of these IoT devices have default passwords and that 75% of them are running insecure software that has not been updated (and in many cases, cannot be updated) and we have a big big problem.

It is not just nation states and organized crime that are abusing these insecure IoT devices and their connectivity to do harm to people and companies and industries across the globe. We must also deal with tech-savvy teenagers breaching the security of billion-dollar companies just for the sake of doing so. Ransomware investigators now bring high school guidance counselors on to their teams to help negotiate and settle payment terms. One might simply call this aspect to the problem the "democratization of crime" where tools once available only to well-funded nation state actors like the NSA and others are now commonly available to anyone, placing the power of orchestrating complex cyber-attacks from the comfort of a couch instead of an operations center.

Tools once available only to well-funded nation state actors like the NSA and others are now commonly available to anyone, placing the power of orchestrating complex cyber-attacks from the comfort of a couch instead of an operations center.

Advanced Materials

The development and use of advanced materials, such as composites and nanomaterials, contribute to the creation of lighter, stronger, and more durable products. These materials often result in improved performance and energy efficiency.

Combining materials discovery with AI and robotics, we see exponential growth in the registration of new compounds and molecules from labs that not only declare such new substances as theoretically possible, but which are being automated and set up to actually synthesize them as well. Google has pioneered something they are calling an "autonomous lab" called DeepMind which has added nearly 400,000 new compounds. Over the course of 17 days of work, DeepMind successfully created 41 out of 58 attempted compounds. A human researcher normally spends months investigating the creation of just one new compound.

Digitalization

The digital transformation of manufacturing processes involves the use of digital technologies to streamline operations, enhance communication, and improve collaboration. Digitalization also facilitates the integration of various systems across the supply chain. It changes long-held business models which did not previously value the use of data or accounted for investment in internal and external capability and needed workforce development. Digitalization also physically reshapes the location and use of facilities and equipment assets relative to people when machine and human productivity changes.

This includes reshaping supply chains when demand changes.

Playing devil's advocate here for a moment can be helpful. Not all digitalization can be characterized as an unqualified "good thing." Sometimes digitalization is actually a solution in search of a problem or a problem itself. Take, for example, a story where quality controls and digitalization of a company's manufacturing process were demonstrating some "issues" that resulted in a production line problem. Let us suppose the company makes a ceramic widget and for some reason, boxes were being shipped that did not contain the purchased widget.

The plant manager engaged the services of a technology consulting firm that introduced weight sensors, lasers, and computer vision technology to inspect the production line. After several hundred thousand dollars of troubleshooting and technology upgrades and enhancements, one of the operators on the line suggested that they place a $30 box fan near the end of the production line. It blew the empty boxes off the rollers and solved the problem of shipping empty boxes to customers. The lesson learned here is twofold: 1) not every problem requires a digital solution and 2) trust in the wisdom of your shop floor operators. We can sometimes find ourselves trying to "over engineer" a solution if we are not careful.

Supply Chain Integration

Advanced manufacturing relies on a tightly integrated and optimized supply chain. Technologies like blockchain can enhance transparency, traceability, and security in the supply chain, reducing inefficiencies and risks.

One of the major lessons learned from the Evergiven incident in the Suez Canal in 2021 was that supply chains are ecosystems. A supply chain is not three links long (you, your upstream and your downstream providers). If we are to have resilience in our economy and avoid disruptions caused by geopolitical events, acts of God/Mother Nature and malicious attacks by nation states looking to cause economic damage and, in some cases, loss of life, then we must expand the scope of our supply chain monitoring and dependency analysis. The more that we aim to maintain low inventory of parts and components for "just in time" manufacturing, the more prone to disruption of that workflow and tightly integrated processes.

> **The more that we aim to maintain low inventory of parts and components for "just in time" manufacturing, the more prone to disruption of that workflow and tightly integrated processes.**

If your product requires components from a semiconductor manufacturer in the Asia Pacific region then you will need to keep close tabs on the supplies and capacity of their operations. While this has always been true even during the 3rd industrial revolution, it is even more pronounced now given some of the geopolitical instability in the region. Recent efforts by the US government to "nearshore" and "onshore" chip fabrication capacity with the CHIPS Act of 2022 clearly demonstrate that strategic thinking is focused on supply chain diversity and shifting research and production capacity to new geographies.

Skilled Workforce

A skilled and adaptable workforce is crucial for the successful implementation of advanced manufacturing technologies. Continuous training and upskilling programs help workers stay abreast of technological advancements and contribute to the industry's growth.

So-called upskilling and cross-skilling of the workforce are critical efforts to avoid having a delayed adoption of new advanced technologies. In addition to simply supporting new ways of manufacturing that take advantage of emerging technologies, we also need to find ways to proactively address the shortage of cybersecurity talent. As we have seen in the previous sections of this chapter, cybersecurity and data management talent is vital to having a robust and resilient advanced manufacturing industry in the US and elsewhere.

Take, for example, the abacus and the electronic calculator. Humans perform mathematical calculations, and we use tools to accomplish these tasks with efficiency, reliability, and speed. The introduction of the abacus 2700 BCE did not stop people from doing math just as the introduction of the electronic calculator in the 1970s did not do away with mathematics skills. It merely transferred some of them to a device that assists humans doing the more interesting mathematics. It can seem a bit scary, but adopting a growth mindset and embracing an attitude of lifelong learning is liberating and empowering.

It is not uncommon for AI, robotics, and automation to be viewed as a threat to human-powered jobs and tasks. But these technologies should be seen as helpful to providing meaningful work. The mundane and repetitive tasks performed by human labor throughout the 1st, 2nd, 3rd and now also the 4th industrial revolution can be relegated to robots, algorithms, and AI.

Regulatory Environment

Government policies and regulations also play a role in cybersecurity resilience. Supportive policies that encourage innovation, research and development, and investment in advanced manufacturing can foster growth in the sector.

U.S. Government Institutes

The U.S. Government has established three Manufacturing USA Institutes that act as national public-private partnerships to build critical mass and direction for U.S. advanced manufacturing in the digitalization of the industry:

- CESMII, The Clean Energy Smart Manufacturing Innovation Institute sponsored by the Department of Education with its program home and headquarters at UCLA.
- MxD, Manufacturing times Digital, sponsored by the Department of Defense.
- CyManII, The Cybersecurity Manufacturing Innovation Institute, sponsored by the Department of Education with its program home and headquarters at Texas Tech.

The U.S. government has also recently announced plans to establish two new Manufacturing USA Institutes sponsored by NIST that bear on strategic roles for data, modeling and the vision of manufacturing as a fully integrated cyber-physical industry:

- The Digital Twin Institute in Semiconductor Manufacturing
- The AI Institute for Resilient Manufacturing

It is incumbent on the private sector to explain these technological advancements to keep regulatory agencies and governance informed on the future.

Traditionally this was inexorably linked to land, sea, air, or space. But in cyberspace, the theater of operations is entirely man-made. There are no natural features or contours in cyberspace upon which to base your tactics and efforts. The remarkable part of his talk, however, was about how there is still this important concept of “the main body” when fighting a war or defending critical infrastructure. All other units and commanders are enlisted in a battle to support the main body. And the main body of the US is the engine of our economy, which rests with the private sector. If the government should ever confuse itself and think that it is the main body, then we are in big trouble. Regulatory agencies would do well to avoid talking about the how in thinking of requirements and compliance frameworks. They can certainly shape the why and the what for the energy sector, water sector, transportation, and other critical infrastructure sectors. But they should only ask questions about the how and leave the how up to the asset owners and operators as they know best what is possible, what is prudent and what is practical.

Global Competition

The competitive landscape on a global scale influences advanced manufacturing. Nations strive to maintain or enhance their competitiveness by investing in technology, research, and development to stay ahead in the global manufacturing arena.

You may have heard the phrase “think globally, act locally” as it relates to environmental action and climate change. The Fourth Industrial Revolution is, almost by definition, linked to sustainability and issues of equitable resource allocation, energy management (peak oil for example), carbon footprint and renewable sources of materials that respect the potential for finding balance among competing forces in the global consumption of scarce resources.

We might laugh now at the Onion’s mock headline for the First Industrial Revolution boasting the “blackened skies of progress” from coal-burning factories, foundries, and power plants. But global commerce back then consisted of forcibly “taking” the land and resources of less developed nations through military conquest and “coca-colonization” as it has been called. Some remnants of the thinking of that era continue, however, to this day and age. Where modern economic coercion causes some countries to remain relegated to third-world status as they sell the next 50 years of their land rights and natural resources to more-developed nations whose economies and plans for growth for their burgeoning populations present them with little choice to retain these rights for themselves.

Here it is worthwhile to mention the World Economic Forum Global Lighthouse Network. Just as we must embrace failure, so too must we study and learn from the successes of others. Imitation is the most sincere form of flattery as Oscar Wilde once said. This community of manufacturers has shown strong leadership in using Industry 4.0 technologies to transform factories, value chains and business models, for compelling financial and operational returns. We note, however, that this network is populated with more international companies than US companies. For all of our innovation and acceptance of failure as the secret to success, we are not represented to the degree that one might expect in the Lighthouse Network. This fact should serve as a call to action and an area for improvement.

Environmental Sustainability

Increasing emphasis on sustainability and environmental considerations is shaping manufacturing practices. The adoption of cleaner and more sustainable manufacturing processes is becoming a priority.

The 2023 UN General Assembly was accompanied by the annual science summit where the UN SDGs (Sustainable Development Goals) are discussed and advanced in the context of science programs and research around the world. At least 5 of the 17 SDGs could (and should) be applied to the cybersecurity and IT industry. Does the term “green cybersecurity” have a place in the market?

In summary, our collective ability to adapt and leverage these myriad factors and adjacent topics will determine the success and competitiveness of manufacturing industries in the future.

Focus on Resilience

What is resilience? Sometimes defined as an object's ability to return to its normal shape after being subjected to force or extreme conditions. Our preferred definition is less about restoring a service or business function than it is about being improved by the event.

This first expression of the term originates in engineering uses of the word in relation to tensile strength and ductile properties. But it was also introduced in ecology and psychology where the concept is less concerned with returning to a former state than it is with adapting and coping with extreme conditions or forces.

Cyber resilience is a more recent incantation of the term and can do well to understand its uses in other domains such as education as well as war. An old Chinese proverb "A tree that is unbending is easily broken" originally occurred in the religious classic, the Tao Te Ching, with the commentary that "The hard and strong will fall, the soft and weak will overcome". The fable, however, is used to deliver different messages in different times with cowardice being attributed to the willow at some points in history, but generally the lesson learned is that the willow survives the storm whereas the mighty oak does not. Nicholas Taleb has a book entitled "Antifragile" where he talks about how bones are strengthened when subjected to stress.

To focus on resilience is to:

- Assume breach
- Embrace failure, not fear it
- Seek indicators of: (Robustness, Adaptability, Transformability)

Embracing Failure as an Advantage

Some cultures stigmatize failure much more than in the US. Singapore and Japan are two such examples where innovation is actually held back because of cultural norms around success and failure. The evolution and advancement of technology often requires taking risks and embracing failure. US companies enjoy an advantage because of our cultural attitude towards failure and that embracing failure is one of the core strengths of our system.

> **US companies enjoy an advantage because of our cultural attitude towards failure and that embracing failure is one of the core strengths of our system.**

> **"If you look at the most successful economy in the world, the American economy, you ask yourself, why are they so successful?**
>
> **One of the reasons is that there's a general culture of accepting honest failure. If you fail you're not stigmatised as you are in Singapore. If you fail in Singapore, you're finished. But in America if it's an honest failure, people don't stigmatise you. They expect you to get up and try again. Try until you succeed. That's the culture we want."**
>
> **Tommy Koh,**
> Singapore's Ambassador At Large and negotiator of the US-Singapore Free Trade Agreement (USSFTA)

We need to have a model for resilience which encourages the creation of robust, fault-tolerance systems. Trustworthy systems that are hardened and improved when subjected to force and attacks. We cannot merely think of disaster recovery and business continuity planning as efforts to return to the state prior to a breach or attack. Why? Because the system was vulnerable and exposed before the attack. We must find ways to transform and adapt our critical infrastructure to have cybersecurity resilience be a real capability.

To cast off the shackles of mindless adherence to the ritual of compliance as dutifully practiced by thousands of auditors and accountants, we must focus on resilience. Resilience assumes failure just as cybersecurity must assume compromise. The attackers will bypass your tools and training, of that you can be certain. We must accept and embrace failure, not fear it.

Navigating the Impact of Cybersecurity on Labor Dynamics

Cybersecurity demands us to think differently. As technology advances, systems become more connected and more data is captured, we must continuously evolve to counter sophisticated threats, requiring a proactive and adaptive mindset. Protecting digital assets involves not only technical skills but also strategic thinking and vigilance across all organizational levels. Cybersecurity significantly impacts the workforce by influencing how employees interact with technology, handle sensitive information, and collaborate with colleagues, fundamentally altering traditional approaches to workforce training and operations. This call to action will drive the demand for a range of skills that may not exist today.

A strong cybersecurity framework ensures that employees are aware of potential threats, follow best practices for data protection, and adhere to security protocols to safeguard company assets. In the event of a cyberattack or data breach, the workforce may experience disruptions in workflow, loss of productivity, and potential damage to the organization's reputation. Additionally, cybersecurity measures can impact employee morale and job satisfaction, as stringent security policies may create barriers to accessing certain tools or systems. Overall, a robust cybersecurity strategy is essential for protecting both the workforce and the organization from potential cyber threats and ensuring a secure and productive work environment.

Leaders must also consider customer expectations and satisfaction regarding cybersecurity. Our workforce will need to understand and address the evolving needs of consumers to ensure they feel secure. What skills require emotional intelligence in cybersecurity workforce development? Staying ahead of emerging trends is imperative, making it crucial to equip the workforce with the ability to detect potential threats through collaboration with AI and digital tools.

Innovative thinking will be a necessary skill. The skill for innovative thinking in cybersecurity involves the ability to think critically, creatively, and strategically to anticipate and respond to evolving cyber threats. This includes staying updated on the latest trends and technologies in cybersecurity, thinking outside the box to identify vulnerabilities and potential risks, and developing innovative solutions to protect data and systems from cyberattacks. Additionally, having strong problem-solving skills, attention to detail, and a willingness to experiment with new approaches are essential for fostering innovative thinking in cybersecurity.

By continuously challenging assumptions, exploring new ideas, and adapting to changing threats, cybersecurity professionals can effectively enhance their innovative thinking skills to stay ahead of cyber threats and protect sensitive information.

Guiding Principles for Integrating Cybersecurity

1. Cybersecurity's Workforce Impact

Cybersecurity influences how employees interact with technology, handle sensitive information, and collaborate, requiring adherence to data protection protocols to safeguard company assets and ensure a secure work environment.

2. Customer-Centric Strategy

Meeting customer expectations is central to cybersecurity strategy, necessitating that the workforce understands and addresses evolving customer needs to maintain trust and a sense of security.

3. Emotional Intelligence in Cybersecurity

Developing cybersecurity skills that require emotional intelligence is crucial, as employees must navigate stringent security policies and maintain morale and job satisfaction.

4. Innovative Thinking

Critical, creative, and strategic thinking are essential for staying ahead of evolving cyber threats. Employees need to be updated on the latest trends and technologies, identify vulnerabilities, and develop innovative solutions.

5. Continuous Learning and Adaptation

Fostering a culture of continuous learning and adaptation is vital. Employees must challenge assumptions, explore new ideas, and adapt to changing threats to enhance their innovative thinking skills and effectively protect sensitive information.

Key Action Items

01

Enhance Data Security Practices

Prioritize the protection of sensitive data by implementing robust security measures across all data management areas: storage, transmission, access, and provenance. Leverage advanced encryption, authentication protocols, and regularly update security frameworks to guard against emerging threats, including potential quantum computing attacks.

02

Optimize Data Management Strategies

Balance the use of cloud-based and on-prem storage solutions to ensure scalability, accessibility, and security. Invest in compatible and modern communication protocols, such as MQTT or OPC UA, to enhance the reliability of data transmission and mitigate the risks associated with legacy systems.

03

Facilitate Workforce Development in Data Security

Invest in education and training programs to equip the workforce with the skills needed to manage and protect data in the digital economy. Support initiatives that foster collaboration between academia, industry, and government to build a skilled workforce capable of addressing modern data security challenges.

04

Transforming the Supply Chain with Blockchain

Sriram Narayanan

Eli Broad Endowed Professor of Supply Chain Management

Michigan State University

Alok Raj

Department of Production
Operations and Decision Sciences

XLRI -Xavier School of Management, Jamshedpur, India

MICHIGAN STATE UNIVERSITY

4.1 INTRODUCTION

Blockchain technology is poised to revolutionize the manufacturing supply chain by enhancing transparency, security, and efficiency across all stages of production and distribution. This chapter explores how blockchain can streamline operations, reduce fraud, and foster trust among partners. As industry rapidly adopts advanced solutions, blockchain will be a criticial enabler to a stronger manufacturing ecosystem.

Blockchain is a decentralized digital ledger that records transactions across a network of computers in a secure and transparent manner. Utilizing cryptographic techniques, each transaction is securely linked to the previous one, forming a chain of blocks that cannot be altered or tampered with. This decentralized nature eliminates the need for intermediaries, reducing the risk of fraud and enhancing trust among participants. With its potential to revolutionize diverse sectors such as finance, healthcare, supply chain, and beyond, blockchain represents a paradigm shift towards greater transparency, efficiency, and decentralization in the digital age. Numerous blockchain-based platforms like IBM Food Trust, Provenance, Dibiz, SkuChain, BlockVerify, Vechain, Factom, Bext360, Ripe.io, BartDigital, BeefChain, and OwlTing are emerging to enhance supply chain operations. Grand View Research reports that the global blockchain market, valued at $3.67 billion in 2020, is projected to reach $394.6 billion by 2028, with an annual growth rate of 82.4%.

By establishing a shared, immutable ledger of transactions, blockchain facilitates real-time tracking of goods from their raw material stage to the final consumer, fostering trust among stakeholders and mitigating risks associated with fraud and errors. A pivotal application of blockchain in supply chains lies in traceability and provenance tracking. Through comprehensive recording of all transactions and movements on the blockchain, companies can readily trace product origins, verify authenticity, and ensure adherence to regulatory standards, a critical feature in industries prioritizing product safety and quality, such as food and pharmaceuticals. Moreover, blockchain streamlines supply chain operations through the implementation of smart contracts. These self-executing contracts automate tasks or payments based on predefined conditions, facilitating seamless transaction processing—such as automatic payment upon goods delivery or penalty enforcement for late shipments—thus enhancing efficiency and reducing administrative burdens.

Although blockchain holds immense promise for supply chain management, its widespread adoption remains in its infancy, hindered by challenges such as scalability, interoperability, and regulatory concerns. Furthermore, companies need to invest in infrastructure, talent, and education to fully capitalize on blockchain's benefits in their supply chains. A primary driver for integrating blockchain into supply chain management is to facilitate secure and efficient information exchange. Unlike conventional methods like enterprise resource planning (ERP), electronic data interchange (EDI), and reliance on third-party intermediaries, blockchain offers distinct advantages. ERP and EDI often incur high integration costs, limiting information sharing to one-to-one relationships—a constraint that escalates with the number of involved firms. Similarly, third-party intermediaries entail significant expenses. However, blockchain's flexibility regarding participant numbers substantially reduces integration costs across multiple organizations. Additionally, blockchain's synergy with the Internet of Things (IoT)—a network of interconnected devices equipped with autonomous sensors and software—enables automated data recording and transfer, facilitating seamless implementation of smart contracts. These contracts, embedded within the blockchain, autonomously execute transactions (e.g., supplier payments) upon meeting predefined conditions (e.g., product delivery). Industry forecasts predict substantial growth, with the global blockchain IoT market projected to reach $2.4 billion by 2026 and the global smart contracts market expected to hit $345.4 million by 2026. These transformative technologies not only enhance transparency in supply chains but also foster innovative contracting and collaboration approaches among firms.

4.2 FUNDAMENTALS OF BLOCKCHAIN TECHNOLOGY

Blockchain technology encompasses several key concepts that are fundamental to its operation and effectiveness in various applications. These concepts include distributed ledger, consensus mechanisms, and smart contracts.

Distributed Ledger

The distributed ledger is the foundational component of blockchain technology. Unlike traditional centralized databases, a distributed ledger is decentralized and spread across multiple nodes or computers within a network. Each node maintains a copy of the ledger, and all copies are updated simultaneously in a synchronized manner. This decentralization ensures that no single entity has control over the entire ledger, enhancing security, resilience, and transparency. Changes to the ledger are recorded in blocks, which are linked together in a chronological chain, forming the blockchain.

Bitcoin blockchain - In the Bitcoin network, the distributed ledger records all transactions of the digital currency Bitcoin. Every participant in the network has a copy of the ledger, and transactions are verified and added to the blockchain through a process called mining.

Consensus Mechanisms

Consensus mechanisms are protocols or algorithms used to achieve agreement among network participants on the validity of transactions and the addition of new blocks to the blockchain. These mechanisms ensure that all nodes in the network reach a consensus or common understanding of the state of the ledger, even in the absence of a central authority.

Proof of Work (PoW) - PoW is a consensus mechanism used in the Bitcoin blockchain. Miners compete to solve complex mathematical puzzles, with the first miner to solve the puzzle earning the right to add a new block of transactions to the blockchain. This process requires significant computational power and serves to secure the network against malicious actors.

Smart Contracts

Smart contracts represent agreements encoded into computer code, capable of self-execution based on predefined rules and conditions. They automate the enforcement of contract terms once specified conditions are met, eliminating the necessity for intermediaries. Notably, the Ethereum blockchain is known for its smart contract capabilities, empowering developers to build decentralized applications (DApps) and programmable digital assets. With smart contracts, various applications emerge, spanning decentralized finance (DeFi), supply chain management, and the tokenization of assets.

4.3 TYPES OF BLOCKCHAINS (PUBLIC, PRIVATE, CONSORTIUM)

Permissionless and permissioned blockchains are two distinct categories that encompass the broader classification of public, private, and consortium blockchains.

Permissionless (Public Blockchains)

Permissionless blockchains, also known as public blockchains, are decentralized networks where anyone can join, participate, and validate transactions without requiring authorization. Participants in permissionless blockchains maintain anonymity, and transactions are transparently recorded on the. In a permissionless blockchain, participants can add information to the blockchain without requiring special permission. However, this does not mean that participants can add information without meeting additional conditions; rather, these conditions cannot be based on the participant's identity. For example, in Bitcoin, a permissionless blockchain, participants must solve a computational puzzle to add information. While this approach provides some security guarantees, it can also lead to inefficiencies, such as prolonged disagreements over the information stored on the blockchain. This ambiguity can be costly in business settings, where clarity and trust are essential. Examples of permissionless blockchains include Bitcoin and Ethereum, where anyone can become a node in the network and participate in the consensus process to validate transactions.

Permissioned Blockchain (Private and Consortium Blockchains)

Permissioned blockchains, also known as private or consortium blockchains, restrict access to authorized participants who are granted permission to join the network. In private blockchains, access is controlled by a single organization, while in consortium blockchains, access is granted to a group of pre-selected participants who collectively manage the network. Participants in permissioned blockchains are known and identifiable, and transactions may be subject to access controls, privacy measures, and governance rules. permissioned blockchains offer several advantages for managing supply chains. They tend to be more scalable, efficient, and customizable, making them better suited for consortiums or industries with shared interests. Examples of permissioned blockchains include Hyperledger Fabric and R3 Corda, which are often used for enterprise applications, supply chain management, and consortium-led initiatives where privacy, scalability, and control are paramount.

In summary, permissionless blockchains prioritize decentralization and openness, allowing anyone to participate without requiring permission. In contrast, permissioned blockchains restrict access to authorized participants and offer greater control, privacy, and scalability. While permissionless blockchains are commonly associated with public blockchains like Bitcoin and Ethereum, permissioned blockchains encompass both private and consortium blockchains deployed for specific enterprise use cases.

4.4 APPLICATIONS OF BLOCKCHAIN IN SUPPLY CHAIN MANAGEMENT

Traceability and Provenance Tracking

Blockchain enables the creation of a transparent and tamper-proof record of every transaction and movement within the supply chain. Each product or batch is assigned a unique digital identity, or a "digital twin," which is recorded on the blockchain along with relevant information such as origin, production details, transportation history, and ownership transfers. This traceability allows stakeholders to track the journey of products from raw materials to the end consumer in real-time. With blockchain, supply chains can verify the authenticity and integrity of products by tracing their provenance back to the source. Stakeholders can ensure compliance with regulations, standards, and ethical practices by recording every step of the production process on the blockchain, including the origin of raw materials, manufacturing conditions, and quality control measures. This transparency also helps identify and address issues such as counterfeit goods, fraud, and unauthorized alterations.

With blockchain, supply chains can verify the authenticity and integrity of products by tracing their provenance back to the source

Walmart collaborated with IBM to implement blockchain technology for traceability in its food supply chain. Using blockchain, Walmart can track the journey of mangoes from farms in Mexico to store shelves in the U.S. in just seconds, compared to days or weeks using traditional methods. This enhanced traceability improves food safety, reduces waste, and strengthens consumer trust. De Beers, the world's leading diamond company, launched "Tracr," a blockchain-based platform to track the provenance of diamonds from mine to market. By recording diamond characteristics, certifications, and transactions on the blockchain, De Beers ensures transparency and authenticity in the diamond supply chain, combating issues like conflict diamonds and unethical practices. VeChain, a blockchain platform specializing in supply chain management, has partnered with various companies across industries to implement traceability solutions. For example, VeChain collaborated with H&M to trace the origin of clothing items, providing consumers with insights into the manufacturing process and sustainability efforts. By leveraging blockchain for traceability and provenance tracking, supply chains can enhance efficiency, mitigate risks, improve compliance, and build trust among stakeholders and consumers.

Supply Chain Visibility and Real-time Monitoring

Supply chain visibility and real-time monitoring are critical components of efficient supply chain management, and blockchain technology offers innovative solutions to enhance these aspects. With blockchain's decentralized and transparent ledger, supply chain stakeholders can gain unprecedented visibility into the movement, status, and condition of goods throughout the entire supply chain network. Blockchain enables real-time visibility into the supply chain by recording every transaction, movement, and event on an immutable ledger accessible to all authorized participants. This transparency allows stakeholders to track product location, quantity, and condition at any point in the supply chain journey. From raw material sourcing to manufacturing, transportation, warehousing, and distribution, every step is recorded on the blockchain, providing a comprehensive and auditable trail of the product's lifecycle.

Supply chains can achieve real-time monitoring of assets and shipments by integrating IoT devices such as sensors, RFID tags, and GPS trackers with blockchain technology. These IoT devices collect and transmit data about temperature, humidity, location, and other environmental factors securely recorded on the blockchain. As a result, stakeholders can monitor the status and integrity of goods in transit, identify potential issues or deviations from expected conditions, and take timely corrective actions to prevent disruptions or losses. Maersk, the world's largest container shipping company, partnered with IBM to develop TradeLens, a blockchain-based platform for global trade. TradeLens leverages blockchain and IoT technology to provide end-to-end visibility and real-time tracking of containerized cargo. By digitizing documentation, sharing real-time shipment data, and enabling secure collaboration among stakeholders, TradeLens streamlines supply chain operations reduces paperwork, and enhances visibility across the entire logistics ecosystem.

Counterfeit Prevention and Product Authentication

Counterfeit prevention and product authentication are critical challenges in supply chain management, particularly in industries where counterfeit goods pose significant risks to consumer safety, brand reputation, and revenue. With its inherent features of immutability, transparency, and traceability, blockchain technology offers innovative solutions to address these challenges effectively. Blockchain's decentralized ledger records transactions in a tamper-resistant and immutable manner. Each transaction, such as the production, packaging, and distribution of goods, is cryptographically linked and time-stamped, creating a transparent and unalterable record of the product's journey through the supply chain. This immutable record ensures the authenticity and integrity of products, making it extremely difficult for counterfeiters to introduce fake or adulterated goods into the supply chain undetected. Blockchain enables end-to-end traceability and transparency by providing a comprehensive audit trail of product movements and transactions across the supply chain. With blockchain, stakeholders can track the provenance of products from their origin to the point of sale in real-time. This transparency deters counterfeiters and allows consumers to verify the authenticity and quality of products before making a purchase, fostering trust and confidence in the brand. Blockchain-based authentication solutions leverage unique identifiers, such as serial numbers, QR codes, or NFC tags, embedded in products to link them to their corresponding digital records on the blockchain. Consumers can scan these identifiers using smartphones or dedicated

By verifying the authenticity of products on the blockchain, consumers can make informed purchasing decisions and avoid counterfeit goods.

apps to access detailed information about the product's authenticity, origin, and manufacturing history. By verifying the authenticity of products on the blockchain, consumers can make informed purchasing decisions and avoid counterfeit goods.

MediLedger is a blockchain platform developed by leading pharmaceutical companies to address the challenge of counterfeit drugs in the pharmaceutical supply chain. By utilizing blockchain technology, pharmaceutical companies can track the provenance and authenticity of pharmaceutical products throughout the supply chain, from manufacturing facilities to pharmacies. This initiative enhances patient safety by reducing the circulation of counterfeit drugs and ensures compliance with regulatory requirements for drug traceability and serialization. MediLedger facilitates secure and transparent transactions among supply chain stakeholders, promoting trust and integrity in the pharmaceutical industry.

Supplier Management and Procurement Optimization

Supplier management and procurement optimization are integral components of supply chain management aimed at enhancing efficiency, reducing costs, and ensuring the quality and reliability of the supply chain. Blockchain technology offers innovative solutions to streamline supplier management processes and optimize procurement practices, enabling organizations to achieve greater transparency, traceability, and trust in their supply chains. Blockchain enables the secure and immutable recording of supplier identities, certifications, and compliance documents on a decentralized ledger. By digitizing and storing this information on the blockchain, organizations can streamline the supplier onboarding process and verify the authenticity and legitimacy of potential suppliers more efficiently. Smart contracts can automate the verification and validation of supplier credentials, ensuring compliance with regulatory requirements and industry standards. Blockchain provides end-to-end visibility and traceability of goods throughout the supply chain, including sourcing raw materials, manufacturing processes, and transportation logistics. By integrating blockchain-based tracking systems, organizations can monitor the movement of goods in real time, identify bottlenecks or disruptions, and proactively manage inventory levels. This visibility enables more accurate demand forecasting, reduces lead times, and enhances supply chain resilience. Smart contracts, self-executing contracts with predefined conditions written in code, automate and enforce procurement agreements between buyers and suppliers. These contracts facilitate the execution of procurement processes, such as purchase orders, invoicing, and payments, without intermediaries. Smart contracts can trigger payments automatically upon completing predefined milestones or delivery of goods, reducing transaction costs, eliminating errors, and improving cash flow management. Blockchain-based supply chain financing platforms leverage the transparency and traceability of blockchain technology to provide innovative financing solutions for suppliers. Blockchain enables faster and more secure financing transactions by tokenizing assets and digitizing trade finance instruments, such as letters of credit and bills of lading. Suppliers can access liquidity based on verified transactions recorded on the blockchain, improving cash flow, and working capital management.

Blockchain provides end-to-end visibility and traceability of goods throughout the supply chain, including sourcing raw materials, manufacturing processes, and transportation logistics.

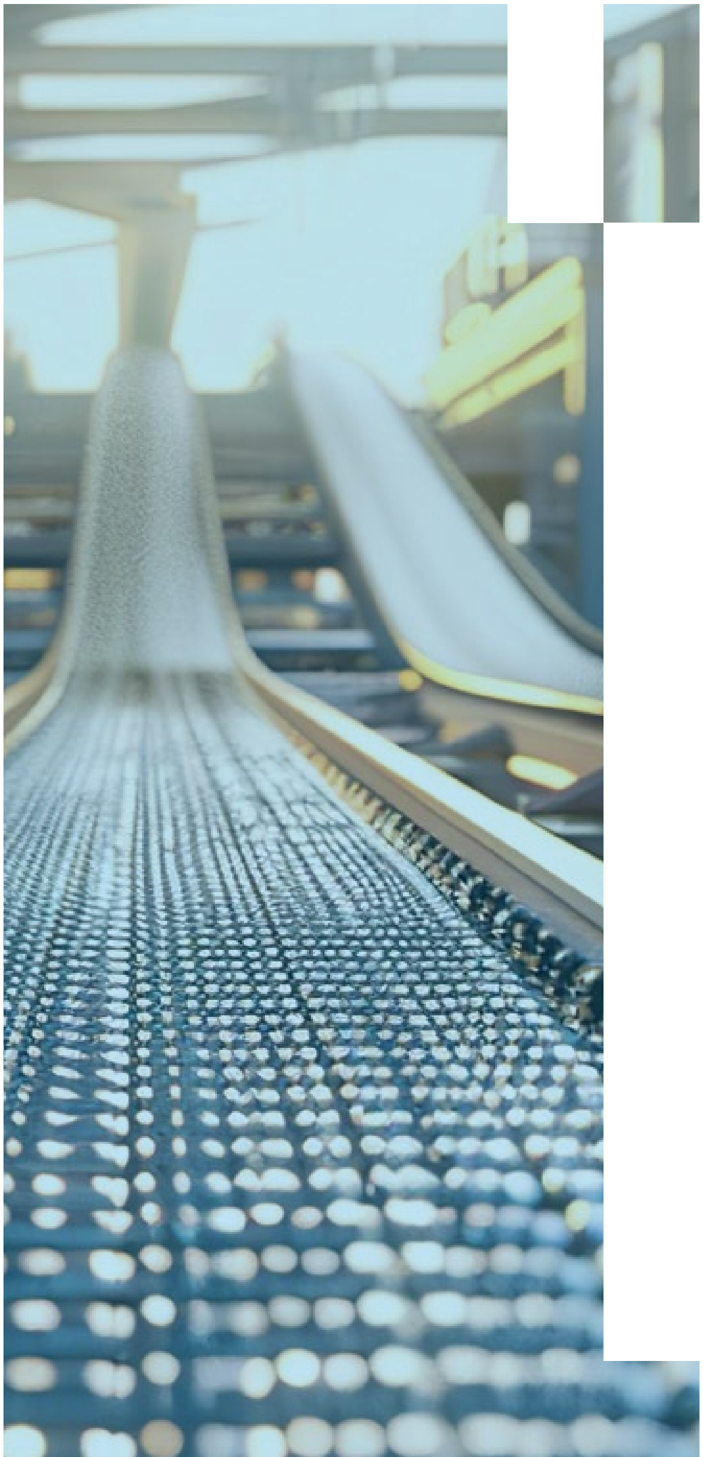
IBM Food Trust is a blockchain-based platform that enables transparent and traceable food supply chains. By digitizing food supply chain data on the blockchain, IBM Food Trust allows retailers, suppliers, and consumers to track the journey of food products from farm to fork. This transparency enhances food safety, reduces food waste, and improves supplier management by providing insights into product quality and compliance. Provenance is a blockchain platform focusing on transparency and traceability in supply chains, particularly in the food, fashion, and pharma industries. The platform enables businesses to track the origin and authenticity of products, verify suppliers' ethical and sustainability credentials, and engage consumers with product stories.

Sustainability and Ethical Sourcing Initiatives

Sustainability and ethical sourcing initiatives are becoming increasingly important for businesses across various industries as they seek to minimize their environmental impact, uphold ethical standards, and meet the growing demand for responsibly sourced products. Blockchain technology offers unique capabilities to enhance transparency, accountability, and trust in supply chains, making it a powerful tool for supporting sustainability and ethical sourcing initiatives. Blockchain enables end-to-end traceability and transparency in supply chains by recording every transaction or movement of goods on an immutable ledger. This capability allows businesses to track the journey of raw materials and products from their source to the end consumer. By providing visibility into each supply chain step, blockchain helps identify inefficiencies, mitigate risks, and ensure compliance with sustainability standards and ethical sourcing practices.

Blockchain can be used to verify the authenticity of certifications and compliance documents related to sustainability and ethical sourcing, such as Fair Trade, organic, or responsible forestry certifications. By digitizing and storing these documents on the blockchain, organizations can prevent fraud and greenwashing and demonstrate their commitment to sustainability and ethical business practices to consumers and stakeholders. Blockchain-based platforms facilitate real-time auditing and monitoring of supply chain activities, allowing businesses to assess their operations' environmental and social impact. Smart contracts can automate supplier compliance verification with sustainability criteria, triggering alerts or notifications when deviations occur. This proactive approach enables prompt corrective actions and continuous improvement in sustainability performance. Blockchain technology enables transparent and accessible communication of sustainability and ethical sourcing information to consumers. By scanning product QR codes or accessing blockchain-enabled platforms, consumers can access detailed information about the product's origin, production process, and sustainability attributes. This transparency builds trust and fosters consumer loyalty, empowering individuals to make informed purchasing decisions aligned with their values.

OpenSC is a blockchain-based platform WWF-Australia and BCG Digital Ventures developed that enables traceability and transparency in food and beverage supply chains . Using blockchain technology, OpenSC tracks the journey of products, such as seafood and agricultural commodities, from farm to fork. By scanning QR codes on product packaging, consumers can access information about the product's provenance, sustainability certifications, and environmental impact. Circulor is a blockchain platform specializing in tracking raw materials, particularly in the mining and automotive industries. Circulor's solution enables companies to trace the origin of minerals, such as cobalt and lithium, used in producing electric vehicle batteries. By ensuring responsible sourcing practices and verifying the absence of conflict minerals, Circulor helps companies meet regulatory requirements and ethical sourcing standards. Provenance is a blockchain platform focusing on transparency and traceability in supply chains, particularly in fashion, cosmetics, and consumer goods. Provenance enables brands to showcase their commitment to sustainability and ethical sourcing by giving consumers access to detailed information about product materials, manufacturing processes, and supply chain partners. This transparency promotes trust and accountability throughout the supply chain. By leveraging blockchain technology for sustainability and ethical sourcing initiatives, businesses can enhance their brand reputation, reduce reputational risks, and contribute to positive social and environmental outcomes. Blockchain drives sustainable and ethical business practices across industries through transparent supply chains and informed consumer choices.



4.5 CHALLENGES AND LIMITATIONS

Scalability Issues and Transaction Throughput

Blockchain networks often face scalability challenges, particularly in terms of transaction throughput and processing speed. As the number of participants and transactions increases, blockchain networks may struggle to efficiently handle the growing volume of data. Scalability issues can lead to delays in transaction confirmation and higher transaction fees, undermining the usability and effectiveness of blockchain technology in supply chains. Solutions such as sharding, layer-two protocols, and consensus algorithm improvements are being explored to address scalability issues and enhance transaction throughput in blockchain networks.

Data Privacy and Confidentiality Concerns

While blockchain technology offers transparency and immutability, it also raises concerns about data privacy and confidentiality. In public blockchains, all transaction data is visible to all participants, raising privacy concerns, especially for sensitive information. Even in permissioned blockchains, where access is restricted, ensuring data confidentiality remains a challenge. Encryption techniques, zero-knowledge proofs, and privacy-enhancing technologies are being developed to address data privacy concerns in blockchain-based supply chain applications.

Integration with Existing Systems and Interoperability

The integration of blockchain technology into existing systems and infrastructure poses complex challenges. Legacy systems often lack compatibility with blockchain protocols, necessitating substantial modifications or upgrades. Furthermore, achieving interoperability among diverse blockchain networks and platforms remains a significant hurdle. To address this challenge, efforts are underway to develop standardization protocols and middleware solutions to facilitate smooth integration and interoperability across disparate systems and blockchain networks.

Regulatory and Legal Considerations

Blockchain technology presents regulatory and legal challenges related to compliance, governance, and jurisdictional issues. Regulations governing data privacy, consumer protection, anti-money laundering (AML), and know-your-customer (KYC) requirements may impact adopting and implementing blockchain-based supply chain solutions. Additionally, legal frameworks for smart contracts, digital signatures, and dispute resolution mechanisms need to be established to ensure legal validity and enforceability of blockchain transactions.

Cost Implications and Return on Investment (ROI)

Implementing blockchain technology in supply chains entails significant upfront costs, including development, deployment, and maintenance expenses. Additionally, ongoing operational costs, such as network fees and infrastructure maintenance, may impact the overall cost-effectiveness of blockchain solutions. Assessing the return on investment (ROI) of blockchain projects requires careful consideration of factors such as efficiency gains, cost savings, risk mitigation, and revenue generation potential. Despite the potential benefits, achieving a positive ROI from blockchain implementations may require overcoming various challenges and optimizing the use of blockchain technology in supply chain operations.

Energy Consumption and Environmental impact

Blockchain networks, particularly those utilizing proof-of-work (PoW) consensus mechanisms like Bitcoin, are criticized for their high energy consumption and environmental impact. The computational power required for PoW consensus algorithms consumes significant electricity, leading to concerns about carbon emissions and environmental sustainability. The energy-intensive nature of blockchain mining operations contributes to the overall carbon footprint of blockchain networks, raising questions about their ecological sustainability. As blockchain technology grows and attracts more users, addressing energy consumption concerns becomes increasingly important. Efforts to develop alternative consensus mechanisms with lower energy requirements, such as proof-of-stake (PoS) and proof-of-authority (PoA), aim to mitigate the environmental impact of blockchain networks. Additionally, initiatives to utilize renewable energy sources for blockchain mining operations and improve energy efficiency through protocol optimizations and hardware innovations are underway to minimize the ecological footprint of blockchain technology. Balancing the benefits of blockchain technology with its environmental impact is essential for promoting sustainable adoption and ensuring the long-term viability of blockchain-based solutions in supply chain management.

Balancing the benefits of blockchain technology with its environmental impact is essential for promoting sustainable adoption and ensuring the long-term viability of blockchain-based solutions in supply chain management.

4.6 IMPLEMENTATION STRATEGIES AND BEST PRACTICES

Implementing blockchain technology in supply chain management requires careful planning and execution. We detail some implementation strategies and best practices to consider:

- Evaluate the organization's readiness for blockchain implementation. Assess the current supply chain processes, technological infrastructure, and organizational capabilities. Identify areas where blockchain can address specific challenges and add value, such as enhancing transparency, traceability, and efficiency. Conduct thorough feasibility studies to evaluate blockchain solutions' viability and potential impact for identified use cases.
- Establish partnerships with key stakeholders across the supply chain ecosystem, including suppliers, manufacturers, distributors, retailers, and technology providers. Collaborate closely with stakeholders to define project objectives, requirements, and success criteria. Leverage consortiums or industry partnerships to pool resources, share best practices and drive innovation in blockchain-enabled supply chains.
- Choose a supplier that aligns with your organization's requirements and objectives. Evaluate factors such as scalability, interoperability, security, and governance capabilities. Consider whether a permissioned or permissionless blockchain suits your use case. Conduct thorough due diligence on potential vendors and consider factors such as reputation, track record, and customer support.
- Start with pilot projects or proofs of concept to test the feasibility and value of blockchain solutions in real-world scenarios. Select a small-scale use case with clear objectives and success criteria. Use agile methodologies to iteratively develop and refine the solution based on feedback and lessons learned. Once the pilot project proves successful, gradually scale up deployment across the organization or supply chain network in phased increments.
- Provide comprehensive training and education to stakeholders involved in blockchain implementation. Ensure that key personnel understand the fundamentals of blockchain technology, its potential applications, and how it will impact their roles and responsibilities. Implement change management strategies to address resistance to change and promote the adoption of blockchain solutions. Foster a culture of innovation and collaboration to drive successful implementation and adoption of blockchain technology in the supply chain.

4.7 FUTURE TRENDS AND EMERGING TECHNOLOGIES

As we look towards the future of blockchain in supply chain management, several trends and emerging technologies are poised to shape its evolution:

Evolution of Blockchain in Supply Chain Management

The role of blockchain in supply chains is expected to continue evolving, with increased adoption and maturation of the technology. We anticipate broader blockchain integration across various industries to enhance transparency, traceability, and efficiency throughout the supply chain lifecycle. As blockchain solutions become more sophisticated, we may see advancements in smart contracts, decentralized governance, and interoperability between different blockchain networks.

Integration with Other Emerging Technologies (e.g., Internet of Things, Artificial Intelligence)

Blockchain will likely be integrated with other emerging technologies, such as the Internet of Things (IoT) and artificial intelligence (AI) to create more intelligent and automated supply chain systems. By combining blockchain with IoT sensors and devices, organizations can capture real-time data on the movement and condition of goods, enabling greater supply chain visibility and predictive analytics. AI algorithms can analyse blockchain data to identify patterns, optimize processes, and make data-driven decisions.

Potential Impact of Quantum Computing on Blockchain Security

The advent of quantum computing poses both opportunities and challenges for blockchain security. While quantum computing has the potential to break existing cryptographic algorithms used in blockchain, it also offers opportunities to enhance security through quantum-resistant encryption techniques. Research efforts are underway to develop quantum-resistant blockchain protocols that can withstand the cryptographic threats posed by quantum computers.

Regulatory Developments and Industry Standards

Regulatory frameworks around blockchain technology are still evolving, with governments and regulatory bodies exploring policies to govern its use in various industries. Industry standards and best practices for blockchain implementation in supply chains are also emerging, facilitating interoperability and collaboration between different stakeholders. As blockchain adoption grows, we can expect to see continued efforts to establish clear regulatory guidelines and standards to ensure compliance and foster innovation.

Overall, the future of blockchain in supply chain management holds tremendous promise, with advancements in technology, regulatory frameworks, and industry collaboration driving its continued growth and impact on global supply chains.

4.8 CONCLUSION

Looking forward, the trajectory of blockchain in supply chain management appears promising, with ongoing technological advancements and increasing industry adoption. Anticipated trends include deeper integration with complementary technologies like IoT and AI, paving the way for more sophisticated and autonomous supply chain systems. Moreover, regulatory frameworks and industry standards are expected to mature, providing clearer guidelines, and fostering broader adoption. As blockchain solutions evolve to become more scalable and adaptable, they have the potential to drive substantial improvements in supply chain efficiency, resilience, and sustainability.

A strategic approach is paramount for organizations contemplating blockchain adoption in their supply chains. Firstly, a comprehensive assessment of readiness should be conducted, identifying areas where blockchain can deliver the most value. This involves evaluating existing processes, identifying pain points, and aligning blockchain initiatives with broader business objectives. Collaboration and partnership models with key stakeholders can accelerate implementation efforts and ensure alignment with industry standards. Organizations should prioritize scalability, security, and interoperability when selecting blockchain platforms and vendors to ensure long-term viability. Pilot projects and phased deployment strategies allow for iterative testing and refinement, mitigating risks and ensuring successful integration into existing workflows. Lastly, investing in training and change management initiatives is essential to foster stakeholder buy-in and facilitate smooth adoption across the organization. By adhering to these recommendations, organizations can harness the transformative potential of blockchain technology to revolutionize their supply chain operations.

As blockchain solutions evolve to become more scalable and adaptable, they have the potential to drive substantial improvements in supply chain efficiency, resilience, and sustainability.

Massachussets Institute of Technology

Creating a healthy environment for SMEs in the Digital Supply Chain Transformation

SMEs play a critical role in major manufacturing supply chains, including aerospace and automotive, as they provide resilience, agility, and creativity for the larger partners in their respective supply chains. yet find themselves under constant pressure from their OEMs and first tier partners, eroding the very capabilities that the OEMs need from them. In this new world of digital supply chains, the adage “companies don’t compete, supply chains do” will play an even more prominent role as the influx of new information shifts the power balance amongst supply chain players.

Unfortunately, there is already evidence that large entities see the new technology as the next wave of wringing concessions from their SME partners, rather than as a basis for building more resilient supply chains that can eliminate actual waste (vs. cost) and provide products and services to customers at a price premium, while acting as an insurance policy to protect against unknown events. This is supported with ample evidence of OEMs failing to act in their own best interest in the long term, not to mention the extensive damage caused to the SMEs and the local economies that depend on them.

How will the overall health of the US supply chain evolve as these new technologies come up against the immutable laws of supply chain dynamics? This fundamentally depends not on the technology, but on the policies, objectives, and mental models of the larger entities in the supply chain. How can the participants in the supply chain work together to prevent a ‘negative sum game’ and ensure the development of a vibrant and resilient supply chain?

Asymmetric Information, Amplified Pain

The short-term benefits realized by the OEMs are often achieved by weaking the long-term resiliency of the supply chain, which may only become apparent under external supply chain stress. As the OEMs force their smaller suppliers into a chronic state of financial malnutrition, they set themselves up for an extended period of financial security and excess margin, only to be followed by acute amplified shocks to stock price, market share, and customer retention.

Given the average age and cumulative value of manufactured goods as a proxy for retained learning within the US SME manufacturing community, it is to be expected for manufacturing SMEs to resist OEM driven adoption measures. Experience with aggressive supply chain cost reduction efforts, adopted throughout the auto industry, and several waves of bankruptcies has served to erode the trust needed for effective sharing of sensitive information required to realize the value of the digital supply chain.

The Technology Has Changed, The Scoreboard Has Not

Time delays in the supply chain are the fundamental drivers of the amplitude and duration of the bullwhip effect. This has played out in practice as large organizations reorganize parts of their supply chains to reduce the impact of long lead-time items and shift production of specialized sub-assemblies closer to product delivery dates.

Clearly, this provides strong financial drivers for major OEMs to shift certain types of production to regions mirroring sales, which would seem to provide US manufacturing SMEs with a much-needed dimension other than price as a competitive lever to engage against global low-cost competitors.

The reduction in production delay results in a systemic improvement in supply chain performance in that overall cost and responsiveness improves. Although improvement occurs at the level of the supply chain, it is measured at the company level via the mechanism of global stock exchanges. Therefore, it is to be expected that large OEMs will seek to extract full measure of the benefits of supply chain transparency, leaving local SMEs at the second- and third-tier levels in an even weaker position. As an analogy, the entire supply chain is now capable of scoring 'from the three-point line', yet only the OEMs are awarded the full three points on the scoreboard.

Understanding the Full Distance Between OEM and SME

Little's Law is often referred to as Newton's Law for supply chains, yet the profound implications are not always recognized. It enables transportation distance to be expressed in the units of time necessary to convert change in production proximity (miles) into lead time reduction (days), which may then be converted into a financial benefit.

However, production time is merely one component of the overall system response time. Taiichi Ohno, widely considered to be the Father of the Toyota Production System, clearly understood this when he defined TPS in terms of the full cash cycle, instead of simply the manufacturing time of an automobile. It would be wise for OEMs to consider the perspective of their smaller suppliers as they extend payment terms, forcing their SME partners to act as bankers as well as manufacturers.

While there are great opportunities in physical co-location of suppliers, the benefit is easily offset by the financial distance created between OEM and supplier. As noted, the pain associated with this institutionalized starvation of smaller players in the supply chain only becomes apparent to the OEM during periods of existential market crisis. Preventive maintenance, proper care of captive suppliers should be evaluated as a very low-cost insurance policy against squeezing out extra pennies to inflate short-term financial performance.

Final Thoughts

Creating a healthy environment for SMEs in the digital supply chain transformation is essential for fostering a resilient and vibrant supply chain. As we navigate the complexities introduced by advanced technologies and real-time data, the focus must remain on equitable collaboration and long-term sustainability. By shifting policies and mental models, OEMs can leverage digital transparency not merely to extract short-term gains but to build robust supply chains that weather external shocks and drive innovation.

Workforce Evolution

Navigating the Impact of Blockchain on Labor Dynamics

Blockchain technology is revolutionizing supply chains by enhancing transparency, security, and efficiency. However, the human element of this transformation is crucial for its successful implementation and sustainability. As blockchain reshapes traditional supply chain operations and introduces new ways of working, industry leaders must thoughtfully manage their labor forces to adapt to these changes.

Blockchain's ability to provide a decentralized and unchangeable record of transactions fosters greater transparency and trust within the supply chain. This transparency demands that employees at all levels understand and trust the technology. Training programs should be implemented to ensure that workers are comfortable and proficient with blockchain applications, fostering a culture of openness and accountability.

The introduction of blockchain technology will create new roles and require new skill sets. Employees will need to develop expertise in blockchain architecture, smart contracts, and data analysis. Upskilling and reskilling programs are essential to prepare the workforce for these emerging roles, ensuring that employees can effectively leverage blockchain technology.

Blockchain enhances collaboration by enabling secure and decentralized real-time data sharing across the supply chain. This can revolutionize remote work by allowing geographically dispersed teams to collaborate seamlessly. Smart contracts and decentralized autonomous organizations (DAOs) facilitate trustless interactions and automate work agreements, increasing flexibility and autonomy for workers. Industry leaders should encourage a collaborative culture where employees are trained to communicate effectively and work together using blockchain platforms, breaking down silos and improving overall supply chain efficiency.

The introduction of blockchain technology will create new roles and require new skill sets. Employees will need to develop expertise in blockchain architecture, smart contracts, and data analysis.

Blockchain also has the potential to transform the gig economy by providing a secure and transparent platform for freelancers to showcase their skills, receive payments, and build reputations. This can lead to fairer compensation, improved job matching, and enhanced trust between employers and freelancers. As the gig economy grows, blockchain can ensure that freelancers are treated equitably and have access to the same opportunities as traditional employees.

Guiding Principles for Integrating Blockchain

1. Invest in Education and Training

Continuous education and training programs are vital to equip employees with the necessary skills to navigate blockchain technology. Offer workshops, certifications, and hands-on training to ensure that the workforce is well-prepared for the transition.

2. Foster a Culture of Innovation

Encourage an innovative mindset by promoting experimentation and embracing new ideas. Create an environment where employees feel empowered to explore blockchain applications and contribute to process improvements.

3. Promote Inclusivity and Engagement

Ensure that all employees, from the C-suite to the shop floor, are included in the blockchain transformation journey. Regularly communicate the benefits and changes brought about by blockchain to keep everyone engaged and informed.

4. Develop Cross-Functional Teams

Form cross-functional teams that include members from different departments to oversee blockchain integration. This approach will ensure a holistic understanding of the technology's impact and foster a more cohesive implementation strategy.

5. Monitor and Adapt

Continuously monitor the impact of blockchain on the workforce and be ready to adapt strategies as needed. Solicit feedback from employees and make adjustments to training programs and processes to address any challenges that arise.

6. Ethical and Social Responsibility

Blockchain technology enables leaders to be more ethical and socially responsible by fostering a transparent and fair work environment. Embrace blockchain's potential to drive innovation, improve efficiency, and create new opportunities for workers, ultimately leading to a strong, diverse-thinking workforce and further technological advancements.

Key Action Items

01

Evaluate and Prepare for Blockchain Implementation

Conduct a thorough readiness assessment of your organization's supply chain processes, technological infrastructure, and capabilities. Identify specific areas where blockchain can enhance transparency, traceability, and efficiency. Undertake feasibility studies to evaluate the potential impact and value of blockchain solutions for targeted use cases.

02

Implement Pilot Projects

Begin with pilot projects or proofs of concept to test blockchain solutions in real-world scenarios. Select small-scale use cases with clear objectives and success criteria. Use agile methodologies to iteratively develop and refine the solution based on feedback. Gradually scale up successful projects across the organization or supply chain network in phased increments.

03

Integrate Blockchain with IoT and AI

Leverage the combination of blockchain, IoT sensors, and AI to enhance supply chain visibility and automation. Capture real-time data on the movement and condition of goods using IoT devices, and employ AI algorithms to analyze blockchain data, identify patterns, optimize processes, and enable predictive analytics for informed decision-making.

Key Takeaways

01

Step-by-Step Approach to Smart Factory Transition

The journey towards achieving a fully functional Smart Factory is a gradual, multi-year process that involves incremental changes. Manufacturing SMEs should transition methodically, and we should recognize that some companies may opt to stop at less advanced stages. For this transition, the importance of a comprehensive blueprint to avoid suboptimal outcomes is paramount, especially given the modularity and decreasing costs of new technologies.

02

Importance of Developing Workforce Skills

Alongside technological advancements, equal emphasis must be placed on developing “smart people” skills within the workforce. This includes educating all levels of employees on smart technology and leadership skills, such as motivation, empowerment, and coaching. Failure to prioritize workforce development could lead to resistance or even sabotage of smart technology initiatives.

03

Addressing Current Disruptions in Manufacturing

There are several key disruptions impacting US manufacturing, such as digital transformation, EV transition, supply chain issues, and workforce challenges. By adopting smart factory practices, manufacturers can enhance their agility and resilience, allowing them to better manage these disruptions. The collaborative effort between manufacturers, government agencies, and technology companies is crucial for accelerating digital transformation and ensuring a robust and competitive US manufacturing sector.

04

Transformative Potential of Industrial AI in Smart Manufacturing

Industrial AI is distinguished from conventional AI by its systematic and disciplined approach, specifically tailored to enhance operational efficiency, reliability, and productivity in smart manufacturing and maintenance. Through detailed case studies on CNC machines, bandsaw systems, and wind farms, the paper illustrates how Industrial AI can significantly improve predictive maintenance and production optimization, leading to repeatable and consistent success.

05

Importance of Multidimensional and Transfer Learning

Multidimensional learning and transfer learning in the evolution of Industrial AI is critical. These advanced learning techniques are essential for addressing the unique challenges and complexities inherent in industrial environments. By integrating domain-specific knowledge, Industrial AI can better navigate and solve industry-specific problems, thereby maximizing its potential impact.

06

Collaborative Effort for Effective Deployment

Addressing challenges such as cybersecurity, data integrity, and model interpretability is crucial for the robust and secure deployment of Industrial AI technologies. A collaborative effort between academia and industry can tackle these issues, ensuring that Industrial AI can be effectively and securely integrated into manufacturing processes. This cooperation is vital for fostering innovation and maintaining the integrity and security of AI-driven manufacturing systems.

07

Intersection of Data Management and Cybersecurity in Advanced Manufacturing

The success of advanced manufacturing and national security hinges on the effective integration of data management and cybersecurity. AI-driven material discovery and tissue fabrication techniques are case studies showing the profound shifts reshaping the manufacturing landscape. The structure and compartmentalization of data will be as imperative in safeguarding manufacturing innovations as the cybersecurity programs that constitute the first line of defense.

08

Global Competition and Environmental Sustainability

Global competition influences the need for advanced manufacturing. Accordingly, nations should invest in technology, research, and development to maintain competitiveness. Sustainability is critical in manufacturing practices, with a focus on equitable resource allocation, energy management, and reducing carbon footprints. The discussion of the World Economic Forum Global Lighthouse Network calls for the US to elevate more factories to this standard, learning from global examples of successful implementation of Fourth Industrial Revolution technologies.

09

Resilience and Embracing Failure

Resilience is defined not just as the ability to return to a previous state but as the capacity to adapt and improve through adversity. There is a need for robust, fault-tolerant systems in cybersecurity, encouraging a shift from mere compliance to true resilience. Embracing failure as an advantage is a cultural strength of the US, fostering innovation and technological advancement. Systems with cyber-resilience may not only recover from breaches, but also become stronger and more secure as a result.

10

Transformative Potential of Blockchain in Supply Chain Management

Blockchain technology is revolutionizing supply chain management by offering unparalleled transparency, traceability, and operational efficiency. Through a decentralized, immutable ledger, blockchain enables real-time tracking of goods from raw materials to the final consumer. This fosters trust among stakeholders, mitigates risks associated with fraud and errors, and addresses challenges such as counterfeit goods, product recalls, and inefficient workflows.

11

Enhancing Operations with Smart Contracts and IoT Integration

The implementation of smart contracts on the blockchain streamlines supply chain operations by automating tasks and payments based on predefined conditions. This reduces administrative burdens and enhances efficiency, such as automatic payments upon goods delivery or penalty enforcement for late shipments. Additionally, the synergy between blockchain and the Internet of Things (IoT) enables automated data recording and transfer, further facilitating the seamless execution of smart contracts and enhancing transparency in supply chains.

12

Challenges and Strategic Adoption of Blockchain

Widespread adoption of blockchain in supply chain management faces challenges, including scalability, interoperability, and regulatory concerns. Organizations need to invest in infrastructure, talent, and education to fully leverage blockchain's benefits. Collaboration with key stakeholders, pilot projects, and phased deployment strategies are recommended to ensure successful integration and scalability of blockchain solutions. Investing in training and change management is crucial to foster stakeholder buy-in and smooth adoption across the organization.

References

FOREWORD

Bureau of Labor Statistics - Manufacturing Employment
https://data.bls.gov/timeseries/CES3000000001?amp%253bdata_tool=XGtable&output_view=data&include_graphs=true

Federal Reserve - Industrial Production and Capacity Utilization
https://www.federalreserve.gov/releases/g17/current/table7.htm

The Manufacturer - Manufacturing Top Target of Record-breaking Cyber Extortion
https://www.themanufacturer.com/articles/manufacturing-top-target-of-record-breaking-cyber-extortion/

1 PURDUE

Purdue Dauch Center
https://business.purdue.edu/centers/dcmme/

Rockwell Automation/ PLEX – 8th Annual State of Smart Manufacturing
https://www.plex.com/sites/default/files/2023-03/Rockwell-PLEX_8th_SOSM_Report_2023_ENGUS.pdf?tcid=1211

Purdue Dauch Center – Pain or Gain? The EV Options in Indiana & Beyond
https://business.purdue.edu/centers/dcmme/ev-research/reports/manufacturing_pain_or_gain_2021.pdf

Rockwell Automation - 9th Annual State of Smart Manufacturing
https://www.rockwellautomation.com/en-us/capabilities/digital-transformation/state-of-smart-manufacturing.html

SMART MANUFACTURING THE NEW NORMAL: A TP3 Strategy
https://www.amazon.com/SMART-MANUFACTURING-NEW-NORMAL-Strategy/dp/B08GLST6TW

HubSpot – 6 Unique Ways 5G Will Impact the Future of Customer Service
https://blog.hubspot.com/service/5g-customer-service

Cummins – I am a Collaborative Robot. I am Manufacturing
https://www.cummins.com/news/2018/09/04/i-am-collaborative-robot-i-am-manufacturing

Ford – Ford Commits to Manufacturing Batteries
https://corporate.ford.com/articles/electrification/ford-commits-to-manufacturing-batteries.html

2 MARYLAND

World Economic Forum - Fourth Industrial Revolution
https://www.weforum.org/focus/fourth-industrial-revolution/

Industrial Artificial Intelligence
https://arxiv.org/abs/1908.02150

Industrial AI: Applications with Sustainable Performance
https://www.amazon.com/-/he/Jay-Lee/dp/9811521468

Aspentech - Industrial Digitalization
https://www.aspentech.com/en/cp/industrial-digitalization

A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems
https://www.researchgate.net/publication/269709304_A_Cyber-Physical_Systems_architecture_for_Industry_40-based_manufacturing_systems

Internet of Things in Industries: A Survey
https://ieeexplore.ieee.org/document/6714496

Recent advances and trends in predictive manufacturing systems in big data environment
https://www.academia.edu/69704292/Recent_advances_and_trends_in_predictive_manufacturing_systems_in_big_data_environment

A survey of Cyber-Physical Systems
https://ieeexplore.ieee.org/document/6096958

Industrial Big Data Analytics and Cyber-physical Systems for Future Maintenance & Service Innovation
https://www.sciencedirect.com/science/article/pii/S2212827115008744

Cloud manufacturing: A new manufacturing paradigm
https://www.researchgate.net/publication/241709205_Cloud_manufacturing_A_new_manufacturing_paradigm

Cloud manufacturing: Strategic vision and state-of-the-art
https://www.sciencedirect.com/science/article/abs/pii/S0278612513000411

A Unified Framework and Platform for Designing of Cloud-Based Machine Health Monitoring and Manufacturing Systems
https://www.academia.edu/24217184/A_Unified_Framework_and_Platform_for_Designing_of_Cloud_Based_Machine_Health_Monitoring_and_Manufacturing_Systems

Industrial Artificial Intelligence for Industry 4.0-based Manufacturing Systems
https://www.researchgate.net/publication/327557176_Industrial_Artificial_Intelligence_for_Industry_40-based_Manufacturing_Systems

Industrial AI and Predictive Analytics for Smart Manufacturing Systems
https://www.researchgate.net/publication/342246767_Industrial_AI_and_Predictive_Analytics_for_Smart_Manufacturing_Systems

Berkeley Lab - Google DeepMind Adds Nearly 400,000 New Compounds to Berkeley Lab's Materials Project
https://newscenter.lbl.gov/2023/11/29/google-deepmind-new-compounds-materials-project/

The waves that make the pattern: a review on acoustic manipulation in biomedical research
https://www.sciencedirect.com/science/article/pii/S2590006421000181

Cuneiform tablet
https://en.m.wikipedia.org/wiki/File:Cuneiform_tablet-_private_letter_MET_DP-13441-003.jpg

CMS Wire - 6 Critical Success Factors for the Data Strategist
https://www.cmswire.com/digital-experience/6-critical-success-factors-for-the-data-strategist/

National Security Agency - Quantum Computing and Post-Quantum Cryptography
https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF

Office of the Director of National Intelligence - Trusted Data Format
https://www.dni.gov/index.php/who-we-are/organizations/ic-cio/ic-technical-specifications/trusted-data-format

NIST - Towards Resilient Manufacturing Ecosystems Through Artificial Intelligence – Symposium Report
https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.100-47.pdf

CESMII - The 15th Anniversary of Smart Manufacturing
https://www.cesmii.org/the-15th-anniversary-of-smart-manufacturing/

World Economic Forum - Global Lighthouse Network: Transforming advanced manufacturing
https://www.weforum.org/impact/advanced-tecnologies-manufacturing-factories-scaling-innovations/

Verizon - 2023 Verizon Data Breach Investigations Report
https://www.verizon.com/business/resources/reports/dbir/2023/industries-intro/manufacturing-industries/

World Economic Forum - Fourth Industrial Revolution Beacons of Technology and Innovation in Manufacturing
https://www3.weforum.org/docs/WEF_4IR_Beacons_of_Technology_and_Innovation_in_Manufacturing_report_2019.pdf

MFAG - ISAC - Manufacturing Information Sharing and Analysis Center (MFG-ISAC) Launched to Protect the U.S. Manufacturing Sector from Malicious Cyberactivity
https://www.mfgisac.org/news/manufacturing-information-sharing-and-analysis-center-mfg-isac-launched-to-protect-the-us-manufacturing-sector-from-malicious-cyberactivity

Train Orders - Con Ed Finally Ends DC Service
https://www.trainorders.com/discussion/read.php?11,1541316

Statista - Leading countries by number of data centers as of March 2024
https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country/

CHIPS and Science Act
https://en.wikipedia.org/wiki/CHIPS_and_Science_Act

Sustainable Development Goals
https://en.wikipedia.org/wiki/Sustainable_Development_Goals

Medium - The Red Pill of Resilience in InfoSec
https://medium.com/@kshortridge/the-red-pill-of-resilience-in-infosec-65f2c5d5e863

Antifragile: Things That Gain from Disorder
https://www.goodreads.com/book/show/13530973-antifragile

National Association of Manufacturers
https://nam.org/manufacturing-in-the-united-states/facts-about-manufacturing-expanded/

4 MSU

International Journal of Intelligent Systems and Applications - Blockchain with Internet of Things: Benefits, challenges, and future directions.
https://doi.org/10.5815/ijisa.2018.06.05

Supply chain traceability using blockchain. Operations Management Research
https://doi.org/10.1007/s12063-023-00359-y

OM Forum—Distributed Ledgers and Operations: What Operations Management Researchers Should Know About Blockchain Technology. Manufacturing & Service Operations Management
https://doi.org/10.1287/msom.2018.0752

Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption
https://doi.org/10.1109/DCOSS52077.2021.00083

Scaling Blockchains: Can Committee-Based Consensus Help? Management Science
https://doi.org/10.1287/mnsc.2022.03177

Traceability of Ready-to-Wear Clothing through Blockchain Technology. Sustainability
https://doi.org/10.3390/su12187491

Supply chain re-engineering using blockchain technology: A case of smart contract-based tracking process
https://doi.org/10.1016/j.techfore.2019.03.015

Decentralized data access control over consortium blockchains
https://doi.org/10.1016/j.is.2020.101590

Supply Chain Transparency and Blockchain Design. Management Science
https://doi.org/10.1287/mnsc.2023.4851

A Survey of Mathematical Programming Applications in Integrated Steel Plants
https://doi.org/10.1287/msom.3.4.387.9972

Blockchain technology in supply chain operations: Applications, challenges and research opportunities
https://doi.org/10.1016/j.tre.2020.102067

Real-time supply chain—A blockchain architecture for project deliveries
https://doi.org/10.1016/j.rcim.2019.101909

Economics of Permissioned Blockchain Adoption
https://doi.org/10.1287/mnsc.2022.4532

Managing a blockchain-based platform ecosystem for industry-wide adoption: The case of TradeLens
https://doi.org/10.1016/j.techfore.2022.121981

Applications of distributed ledger technology (DLT) and Blockchain-enabled smart contracts in construction
https://doi.org/10.1016/j.autcon.2021.103955

Blockchain Governance—A New Way of Organizing Collaborations?
https://doi.org/10.1287/orsc.2020.1379

The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work
https://doi.org/10.1109/QRS-C55045.2021.00168

PR Newswire - Smart Contracts Market Size to Reach USD 345.4 Million by 2026 at CAGR 18.1%
https://www.prnewswire.com/in/news-releases/smart-contracts-market-size-to-reach-usd-345-4-million-by-2026-at-cagr-18-1-valuates-reports-832536081.html

Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap
https://doi.org/10.1016/j.tre.2022.103012

Blockchain for drug traceability: Architectures and open challenges
https://doi.org/10.1177/14604582211011228

Applying blockchain technology to ensure compliance with sustainability standards in the PPE multi-tier supply chain
https://www.tandfonline.com/doi/abs/10.1080/00207543.2022.2025944

Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends
https://doi.org/10.1109/TSMC.2019.2895123

Blockchain Enabled Data Sharing in Supply Chains: Model, Operationalization, and Tutorial
https://doi.org/10.1111/poms.13356

Harvard Business Review - Building a Transparent Supply Chain
https://hbr.org/2020/05/building-a-transparent-supply-chain

WWW.USC4AM.ORG

The US Center for Advanced Manufacturing drives state, regional and national initiatives that accelerate and strengthen advanced manufacturing in the US, while helping to inform the global manufacturing agenda.

As a community, we ignite potential by harnessing the power of the people and technology through our work. We strive to build an ecosystem that accelerates change to transform manufacturing as a whole by fostering global action borne from local identity.

We are an innovative voice for change in advanced manufacturing for the United States.

US
Center for
Advanced
Manufacturing