McKinsey & Company

Leveraging Industrial IoT and advanced technologies for digital transformation

How to align business, organization, and technology to capture value at scale

by Andreas Behrendt, Enno de Boer, Tarek Kasah, Bodo Koerber, Niko Mohr, and Gérard Richter

Preface

The set of advanced technologies in the manufacturing space is comprised of many digital innovations: advanced analytics, automation, the Industrial Internet of Things (IIoT), Industry 4.0, machine learning, artificial intelligence (AI), cloud platforms, and so on. These innovations have the potential to boost the productivity of companies' legacy operations. For incumbent companies, these advanced technologies support the creation of all-new, digitally enabled business models and help increase operational efficiencies and the customer experience in production and logistics. Manufacturing enterprises that want to modernize cannot ignore these benefits; several large organizations in this space are already working with these technologies, at least to some extent.

Of the digital technologies listed above, IIoT or Industry 4.0, terms used interchangeably in this report, are of particular relevance to manufacturing. Yet while many manufacturing organizations are piloting digital initiatives, very few have managed to scale their IIoT-enabled use cases in a way that achieves significant operational or financial benefits. One of the reasons for this "pilot trap" is probably that IIoT is often regarded primarily as a technical implementation challenge, with the drive for adoption spearheaded by specialists in information technology (IT) and operational technology (OT) functions.

Yet time and again, it becomes apparent that deriving real business gains from IIoT efforts requires top management to create the conditions in which processes across the business can be changed, paving the way for wide-scale, sustainable value creation. For example, connecting production equipment to the internet will allow a company to reduce downtime through analytics-enabled asset productivity optimization, but if the surrounding business processes aren't modified and also optimized, the value is limited to that particular area. In order to maximize IIoT's value, people and processes must also shift to capture the benefits of those data-driven insights by receiving insights in real time to react faster or by gaining better information to drive more targeted action. This requires the commitment of leadership to ensure that IIoT is not just an IT initiative but an organization-wide effort.

Technical obstacles to IIoT at scale exist, too. Many organizations are still wondering, for example, how to overcome the challenges caused by heterogeneous system and application landscapes, or how to analyze which functions should be supported by which systems (for example, product life-cycle management, enterprise resource planning, manufacturing execution, supply-chain management). There is also the question of where those systems should be deployed—on the edge, at the manufacturing site, or in the cloud—a question that relates to the governance between IT and OT and considers latency and security necessities.

Because of these complexities, even companies with a good IIoT track record can be expected to face challenges if they do it alone. Technical IIoT ecosystems are growing and improving by the day. In many cases, collaboration—often with players that have high levels of expertise in areas such as analytics, IIoT, and cloud platforms within the industrial software stack—can be a competitive advantage. Beyond the necessity of collaboration, the complexity of the emerging ecosystems prompts questions concerning investment, leadership, and governance.

Mastering these complexities requires overcoming the integration challenge between business operations, organization, and technology. In this report, we offer guideposts for driving digital transformations by successfully aligning the business, organization, and technology spheres to help manufacturing and technology leaders successfully navigate the IIoT landscape and position their organizations to reap the full set of its benefits.

Contents

Introduction		**6**
Part A:	**Industry trends for a promising perspective on digital manufacturing**	**11**
1	**A brief outline of technological and impact-related developments in the digital manufacturing space**	**11**
1.1	Technology trends are rather promising	11
1.2	Leveraging an IIoT-enabled backbone, the plants in the Global Lighthouse Network achieve significant results in their performance metrics	13
2	**Manufacturing companies should continue to commit to digital innovation, and reassess their digital initiatives**	**17**
Part B:	**A framework for success in IIoT-based value capture at scale**	**21**
1	**Business (Manufacturing)**	**25**
1.1	Use-case identification and prioritization	25
	Step 1: Generate a comprehensive list of use cases in a combined top-down and bottom-up manner	25
	Step 2: Catalog, qualify, and prioritize use cases	25
	Step 3: Set up lighthouse cases for master blueprints	27
1.2	Plant rollout and enablement	28
	Step 1: Set up a rollout that is value driven and pursues impact	28
	Step 2: Start gathering and aggregating data, conducting important activities in parallel	30
	Step 3: Establish the processes and collaboration that enable the required rollout	31
2	**Organization**	**32**
2.1	Value capture: Change and performance management	32
	Step 1: Define an overall road map of the IIoT transformation and use-case target values	32
	Step 2: Set up a value-capture organization, model, and mechanism	32
	Step 3: Implement consistent deviation management	32
2.2	Capability building and a new way of working	33
	Step 1: Establish structural organizational changes and implement new governance and a new way of working	33
	Step 2: Identify and fill the skills gap	36
	Step 3: Manage role transitions and implement a change process to support a mindset shift across hierarchy levels	37

3	**Technology**	**40**
3.1	IIoT and data infrastructure: Core platform design (including IT-OT cybersecurity)	40
	Step 1: Fully assess the current brownfield setup in both OT and IT	46
	Step 2: Create the future target architecture to enable the use case	48
	Step 3: Effectively manage cybersecurity challenges in IT-OT convergence	55
	Step 4: Select a partner rather than a vendor to help implement the platform	59
3.2	IIoT platform: The cloud imperative in manufacturing	59
	Step 1: Make the cloud pay off in the short term	62
	Step 2: Tightly manage and control the cloud transformation	62
	Step 3: Set up an infrastructure team that can operate much like an app development team	64
3.3	Tech ecosystem	64
	Step 1: Understand the key elements of a sustainable ecosystem	65
	Step 2: Choose the right partners, with a view to achieving balanced partner diversity for the platform-enabled ecosystem	65
	Step 3: Implement business development teams as a structure to manage the complex ecosystem and ensure agility	67
Outlook:	**How to get started on a digital transformation in manufacturing**	**68**
Glossary		69
Authors		74

Introduction

Innovations in the industrial software stack, along with applications for advanced analytics, AI, machine learning, 5G connectivity, edge computing, and the Industrial Internet of Things (IIoT), are potentially valuable assets for manufacturers. For many manufacturing companies, however, "tech selection" may be the easy part; capturing value and scaling up impactful use cases is where the challenge lies.

Use cases need to be digitally enabled, but heterogeneous system and application landscapes could be a roadblock deriving from legacy software, organic growth, merger and acquisition activities, and/or decentralized sourcing decisions for solutions and technologies. These technical challenges, in combination with the hurdles of an unclear business plan and insufficient organizational capabilities, end up trapping many companies in an ongoing "pilot purgatory."

In recent years, technology has made tremendous improvements, especially in the field of scalable connectivity and integration, which finally enables manufacturing companies to both wrap and extend their existing solutions, rather than rip and replace them. If used prudently, these technologies allow companies to implement and scale impactful use cases at minimal incremental cost.

In our research and field work, we have observed that industrial manufacturers that take an integrated approach are the most successful. These companies capture the business value of industrial digitization across the value chain, including for their suppliers and customers. From the start of the transformation, they see the importance of the enormous shifts required in organization and technology, which need to be thought through beyond single functions. This report focuses on digital manufacturing as well as the underlying organizational and technological changes to support it (Exhibit 1) .

The goal of this report is to provide deep and ready-to-use insights into the various issues raised by the influx of new technologies as business enablers, and how to successfully capture value and scale use cases in manufacturing. McKinsey's IoT and manufacturing group has launched a research effort to understand the key enablers behind this IIoT-based value capture at scale, and the results are summarized in this report. It provides reasons why companies should continue to leverage IIoT-enabled technology, as well as ready-to-use guidance on how they can do so. The report draws on knowledge from our extensive field work, augmented with the latest McKinsey research and insights from respected sources, including:

— McKinsey studies in partnership with the World Economic Forum, including 54 lighthouses in digital manufacturing[1]

— Experience from major, impactful client studies with leading manufacturing companies on IIoT, analytics, and cloud-enabled transformations, which leverage the latest technologies in connectivity, data architecture, and edge computing

— Key lessons from successful digital and data-driven transformations, with a special focus on skills transformation, capability building, and change management

— McKinsey research and in-depth exchanges with leading academic institutions, industry associations, and industry surveys

This report is not just for IT, OT, and digital executives in the manufacturing environment; it is also relevant for leaders across a variety of functions and areas, including operations, supply chain, process engineering, and services.

---

[1] World Economic Forum and McKinsey & Company, "Global Lighthouse Network: Four durable shifts for a great reset in manufacturing," World Economic Forum, September 2020, weforum.org.

Exhibit 1

Capitalizing on the Industrial Internet of Things requires an integrated approach for driving end-to-end transformation across business, organization, and technology.

Business

Grow revenue		Reduce costs				Optimize cash	
Digital sales and marketing	Digital product design / agile R&D	Digital procurement	Design to cost / design for X	**Digital manu-facturing**	Back-/mid-/ front-office process digitization	Digital supply chain / inventory	Accounts payable and receivable / capex

Focus of this report

Organization

Performance infrastructure: "The brain"	Use a relentless cadence to ensure superior execution and value delivery to the bottom line, driving financial initiatives, objectives, and key results
Financial transparency: "The eye"	Create financial transparency and profit-and-loss-linked value drivers so improvements on the ground translate to financial gain
Change management: "The heart"	Foster the mindset and behavioral changes required to operate in a digitized environment and sustain the transformation
Digital capability building: "The muscle"	Reskill the current organization across leadership, functional, digital, and transformation capabilities
Agile organization: "The yogi"	Build on agile principles to organize, operate, innovate, and transform in a cross-functional and iterative manner

Technology

IIoT infrastructure: "The skeleton"	Develop holistic planning and IIoT architecture to scale digital use cases across the entire organization
Data infrastructure: "The blood"	Get the right data at the right time and quality to enable digital and analytics use cases
Tech ecosystem: "The community"	Expand the network of companies to partner and license with to bring new capabilities to the enterprise

Source: McKinsey Digital Transformation Services

The research and analyses conducted for this report yielded the following key insights:

I. Why manufacturing organizations should leverage IIoT and advanced technologies for their digital transformations

There are multiple strong reasons why companies should begin or continue to leverage IIoT and advanced technologies:

Barriers to IIoT are coming down

— Deployment of use cases at scale is accelerating as platforms become increasingly user-friendly—that is, low-code to no-code software—and tool bundles make development and installation more cost-effective than ever.

— Decentralized computation—from the edge of the shop floor all the way up to the cloud—is becoming mainstream, as infrastructure solutions enable easy management of dispersed networks of platform resources and tackle the issue of real-time requirements.

— Integration and connectivity are critically improved by frameworks such as Open Platform Communications (OPC) Unified Architecture and the arrival of 5G, offering high-speed, low-latency, highly secure, and highly flexible solutions where current alternatives fail.

— Computing and processing power have increased exponentially, while storage and central processing unit costs have fallen dramatically.

Benefits of IIoT are significant

— Significant improvements in productivity, performance, sustainability, agility, speed to market, and customization can be achieved through the right implementation of IIoT, as shown by the World Economic Forum's 54 global lighthouses[2] (see Exhibit 4).

— A shift toward advanced manufacturing significantly increases manufacturers' resilience, allowing them to react more quickly to a crisis through modern digital work-planning tools.

II. How manufacturing organizations can align the business, organization, and technology spheres to capture value at scale

Successful IIoT enablement at scale follows seven key actions across three areas:

— **On the business side.** First, use cases are identified, prioritized, and piloted. Then, the road map to roll out these use cases across IT, OT, and all plant locations, as well as the necessary value capture and capability measures, are defined with overarching impact in view and without distraction by local solution requirements. In terms of continuous improvement of local initiatives, however, these need to be monitored and further pursued.

— **On the organization side.** Clear target values for the entire transformation are set and a unit responsible for monitoring progress and course-correcting as appropriate is installed. Then, a new way of working that facilitates cross-functional engagement and builds relevant skills and capabilities should be put in place.

— **On the technology side.** First, the current situation and the target architecture of the IIoT platform are defined, focusing on the collection, connection, ingestion, and integration of data in ways that enable the use cases—including managing the platform's cybersecurity. Second, the impact of cloud computing in manufacturing needs to be understood and integrated into the overall design of the platform. Third, the ecosystem of vendors and partners to support implementation is set up, factoring in different levels of individual plant complexities (such as manufacturing type and products, plant size, and IT-OT landscape).

---

[2] As of October 2020.

Table 1: Overview of the seven enabling processes of a digital transformation in manufacturing and their key steps.

Dimension	Process	Key steps	Page
Business (Manufacturing)	1.1 Use-case identification and prioritization	— Step 1: Generate a comprehensive list of use cases in a combined top-down and bottom-up manner — Step 2: Catalog, qualify, and prioritize use cases — Step 3: Set up lighthouse cases for master blueprints	25 25 27
	1.2 Plant rollout and enablement	— Step 1: Set up a rollout that is value driven and pursues impact — Step 2: Start gathering and aggregating data, conducting important activities in parallel — Step 3: Establish the processes and collaboration that enable the required rollout	28 30 31
Organization	2.1 Value capture: Change and performance management	— Step 1: Define an overall road map of the IIoT transformation and use-case target values — Step 2: Set up a value-capture organization, model, and mechanism — Step 3: Implement consistent deviation management	32 32 32
	2.2 Capability building and a new way of working	— Step 1: Establish structural organizational changes and implement new governance and a new way of working — Step 2: Identify and fill the skills gap — Step 3: Manage role transitions and implement a change process to support a mindset shift across hierarchy levels	33 36 37
Technology	3.1 IIoT and data infrastructure: Core platform design (including IT-OT cybersecurity)	— Step 1: Fully assess the current brownfield setup in both OT and IT — Step 2: Create the future target architecture to enable the use case — Step 3: Effectively manage cybersecurity challenges in IT-OT convergence — Step 4: Select a partner rather than a vendor to help implement the platform	46 48 55 59
	3.2 IIoT platform: The cloud imperative in manufacturing	— Step 1: Make the cloud pay off in the short term — Step 2: Tightly manage and control the cloud transformation — Step 3: Set up an infrastructure team that can operate much like an app development team	62 62 64
	3.3 Tech ecosystem	— Step 1: Understand the key elements of a sustainable ecosystem — Step 2: Choose the right partners with a view to achieving balanced partner diversity for the platform-enabled ecosystem — Step 3: Implement business development teams as a structure to manage the complex ecosystem and ensure agility	65 65 67

These actions are described in significant detail in the report (for an overview, see Table 1 on the previous page). Manufacturers can set themselves up for success even before they take the first official step by asking themselves honest and critical questions about their goals, digital maturity, organizational readiness, and the challenges they face.

A quick guide for the reader

Time is a rare commodity, and we want you to get the most out of this report. Since many readers are interested in specific topics, we have created a guide that notes the most relevant chapters for each audience.

— For the **CEO,** board member, or general manager who suspects the need for a digital transformation in their company's manufacturing operations but is not exactly sure what to do: first and foremost, read Part A to brief yourself on the latest trends and knowledge on leveraging IIoT technology in a manufacturing context, and to learn about the potential impact from lighthouse factory cases identified by McKinsey and the World Economic Forum. Also read the introduction to Part B for a perspective on our framework for a successful digital transformation in manufacturing.

— For the **COO,** senior leader in manufacturing, or plant manager who is looking for a perspective on the business value of IIoT technology and how to unlock it: read Chapter 1 in Part B to understand how to prioritize digital use cases in manufacturing and roll them out across a network of plants to achieve impact at scale. Also read Chapter 2 in Part B for a perspective on what it takes to conduct a successful digital transformation in manufacturing in terms of capturing the value of digital use cases and building the workforce of the future with the required roles and skills.

— For the **CIO** who firmly believes that IIoT technology can move the business forward but is dissatisfied with the technology's performance so far: start with Chapter 3 in Part B to learn more about how IIoT infrastructure can contribute to improving operational efficiency, how IIoT can benefit the business departments, and how an ecosystem of external partners can drive innovation and technology capabilities.

— For the **CDO** who is seeking the latest knowledge and proven expertise on implementing digital initiatives that enable strategic innovation and business transformation in manufacturing: focus on Part A and Chapter 1 in Part B.

— For the **CTO** who is looking for a fresh perspective on the overarching technology infrastructure of his or her organization, including on key aspects like developing marketable technology, suggesting new technologies to implement, and interacting with external buyers and budgeting: first read Chapter 1 in Part B, then Chapter 3 in Part B.

Part A: Industry trends for a promising perspective on digital manufacturing

Many manufacturers still face challenges with IIoT-based and digitally enabled value capture at scale. Nevertheless, there are many indications that there is great potential in digitization just around the corner, so manufacturing companies should continue to commit to and gear up for digital innovation.

1 A brief outline of technological and impact-related developments in the digital manufacturing space

It has been technologically possible to implement IIoT-based use cases for a couple of years already. What we are witnessing now, however, is the opening up of completely new possibilities for implementing sophisticated, innovative use cases in a streamlined way. What's more, plants in the World Economic Forum's Global Lighthouse Network are demonstrating leading-edge capabilities. If done right, leveraging an IIoT-enabled backbone can lead to game-changing improvements in the performance (metrics) of manufacturing companies—across industries and with a wide range of use cases.

1.1 Technology trends are rather promising

Three top-line IIoT-related technological trends concerning use cases and connectivity technologies can be identified:

I. Deployment of use cases is becoming easier
Use-case deployment is simplified primarily through four developments:

— **Network effects.** IIoT platforms are becoming more user-friendly as software supports the expansion of users. Additionally, as access to IIoT software development expands, greater experimentation will occur, to the benefit of the entire IIoT manufacturing ecosystem.

— **Simplified development.** A rich set of ready-to-use application programming interfaces (APIs) and microservices, (semi-)established communication standards, and available apps and editors with little to no need for writing code make for more cost-effective creation and implementation of use cases. These low-code/no-code platforms offer small and medium-sized businesses access to IIoT software functionality without the need for the coding talent that early adopters had to have.

— **Imprinted scalability.** Routines for fast provisioning and updating of apps in reusable data pipelines, containerization for hardware-agnostic deployment of software on different edge devices, and sophisticated solutions for managing the entire software/hardware stack enable the implementation of DevSecOps[3] methodologies and help rapidly scale platforms across factories and plants.

— **Increasing use-case availability.** Computing and processing power have increased significantly, while storage and central processing unit costs have fallen dramatically (Exhibit 2).

II. Edge computing is becoming mainstream
There are three key factors pushing computational capacity out of the cloud and onto sites: 1) edge technologies have intermittent connectivity, which enables a wider range of features than ones that are fully online, 2) sophisticated devices depend on real-time decision making, and 3) the computational decisions required do not rely on greater computing power. By 2025, edge computing can be expected to represent a potential value of $175 billion to

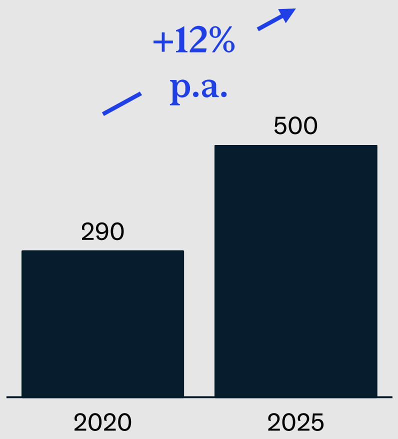
[3] Comprising software development, IT security, and IT operations, DevSecOps extends the established DevOps approach by the important factor of cybersecurity; for further details, see the Glossary.

Exhibit 2

IIoT will be a $500 billion market by 2025 as advances in its essential technologies drive up demand.

High-level estimate

IIoT spending, 2020–25,[1]
USD billions



Overall market expected to grow given strong underlying demand and increasing use-case availability

Key growth drivers

	Early 2000s	Today
Sensor cost	The average unit price per sensor was >USD 1.30	Unit price has fallen to <USD 0.50 per sensor
Data storage cost	Storing 1 GB of data would cost >USD 500	1 GB of data can be stored for as low as USD 0.02
Device ubiquity	IoT devices were largely limited to specialized applications, e.g., security cameras	8.4 bn IoT devices are in use; the average digital consumer owns ~4 connected devices
Connectivity	Phones ran on 2G networks at ~50 kbps; Wi-Fi and Bluetooth were just introduced	The 5G mobile network supports up to 20 GBs (400,000x increase); Wi-Fi and Bluetooth are standard technologies

1. Incl. construction, manufacturing, resource industries, and transportation

Source: IDC; McKinsey analysis

$215 billion in hardware. The industries primarily generating this hardware value are travel, transportation and logistics, and retail, representing approximately 32 percent of current use-case environments.

III. 5G offers manufacturers a connectivity solution where current alternatives fail

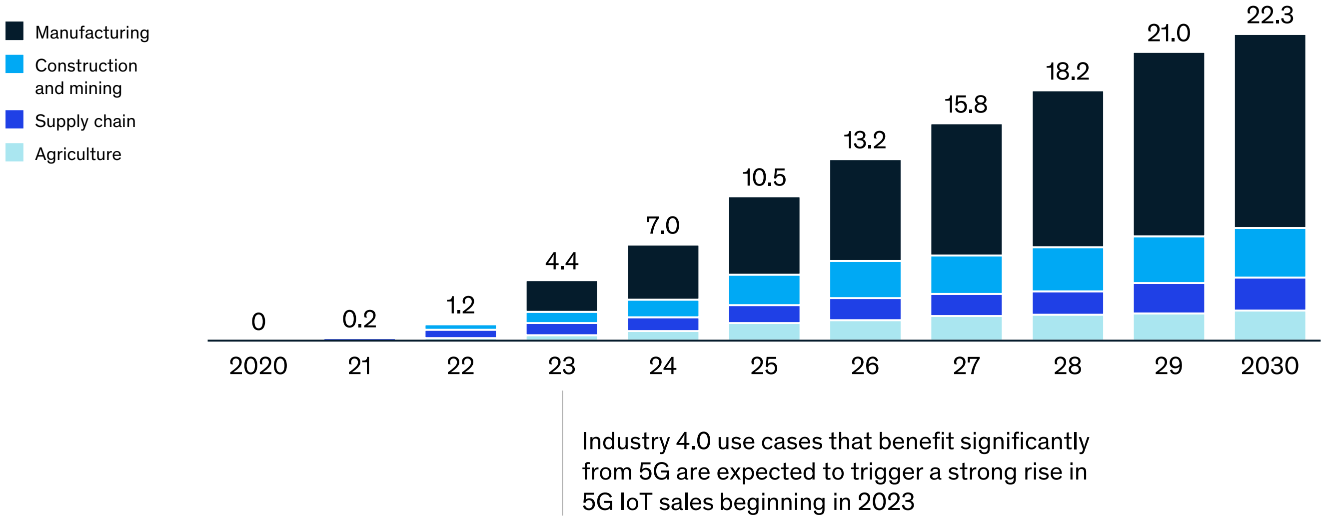
For manufacturers shifting to Industry 4.0, 5G offers relevant short-term opportunities for IIoT. Through this significant step up in performance, factories and plants can overcome the high interference inherent to pre-Industry 4.0 shop floors. As a result, manufacturing is expected to account for over half of all 5G sales for use cases where 5G brings significant benefits (Exhibit 3).

Some of the most compelling use cases for 5G in manufacturing are automated guided vehicles and real-time process control. Today, automated guided vehicles are typically enabled by Wi-Fi and rely on software loaded on the machine to handle routing and task execution. 5G would allow for significantly better connectivity with the edge or cloud for sharing data between vehicles and coordinating fleets in real time, thereby allowing them to break free from fixed paths onto the ever-changing shop-floor environment. As an added benefit, 5G also boosts

Exhibit 3

For Industry 4.0 use cases that benefit significantly from 5G, most 5G IoT hardware unit sales will relate to manufacturing.

Forecast 5G IoT hardware unit sales for Industry 4.0 applications (only business-to-business use cases with significant benefit from 5G), million units



Source: McKinsey analysis

reliability by offering seamless connectivity as the automated guided vehicles move across the factory and jump between access points or radios. When it comes to real-time process control, it has been possible to use wired controllers and sensors for years; however, 5G opens up a new solution space by helping connect modules to conduct targeted sensor-drive analyses relatively easily—this is particularly impactful on old brownfield machines whose control and power systems may be older and less adaptable to modern technologies.

1.2 Leveraging an IIoT-enabled backbone, the plants in the Global Lighthouse Network achieve significant results in their performance metrics

More than 70 percent of companies find it difficult to implement and scale advanced technologies in a way that delivers significant improvement in return on investment or operational key performance indicators (KPIs). Since 2016, the World Economic Forum, in collaboration with McKinsey, has embarked on a journey to identify the front-runners in the adoption of Industry 4.0 technologies and build a network of these successful lighthouses. The aim has been to identify practices and generate insights that would accelerate the adoption of advanced manufacturing technologies. In 2018, over 1,000 production facilities were examined and 16 companies were recognized as leaders in advanced manufacturing. These leaders demonstrate significant results in operational and financial metrics. In 2019, 28 additional facilities were added to what is now known as the Global Lighthouse Network, and 10 more were added in 2020.

What these 54 World Economic Forum lighthouses have in common technologically is an innovative operating system, whose backbone is an integrated IIoT platform that supports and enables integration between business processes and management systems. The lighthouse way of working is often to create a minimum viable product of the IIoT operating system, which can then be replicated and scaled across the company. As these lighthouses first work toward a minimum viable product, agile processes enable iterations early on, before company-level resources must be invested.

The IIoT infrastructure and agile ways of working thus enable the lighthouse factories to add new use cases in minimal time and at minimal cost. As a result, many lighthouses have a wide range of advanced use cases deployed along their supply network, such as end-to-end product development, planning, and delivery, customer connectivity, and digitally enabled sustainability. What all these use cases have in common is the seamless integration of multiple IT systems, such as enterprise resource planning, product life-cycle management, and manufacturing operations management (MOM). MOM is often used interchangeably with MES, which refers to manufacturing execution systems (for further details, see the Glossary).

The impact achieved by manufacturers in the Global Lighthouse Network is unmatched by their peers. The lighthouses were classified as either factories—confined to four walls—or end-to-end facilities, which achieve impact across their value chains. As a factory-level example, a semiconductor factory in Singapore achieved a 22 percent decrease in scrap collected as a result of its IIoT-enabled smart factory. Another example, this time an end-to-end lighthouse, is a production facility for contact lenses whose IIoT-enabled advanced process automation directly led to a double-digit decrease in costs. The impact chart in Exhibit 4 plots the performance of the 54 lighthouses, summarizing the range of financial and operational impact observed in the Global Lighthouse Network.[4]

Ultimately, there will be winners and losers as the shift continues toward Industry 4.0. The speed of adoption of technology has shown to be the variable that puts distance between front-runners, followers, and laggards, with front-runners being the earliest adopters. In 2018, a McKinsey Global Institute analysis projected a remarkable gap between companies that adopt and absorb AI within the first five to seven years and those who lag behind (Exhibit 5). Front-runners, meaning those that have adopted AI technologies, can expect a cumulative 122 percent cash-flow change, while followers may see only a 10 percent cash-flow change. Worse yet, companies that do not adopt AI over the five-to-seven-year horizon are expected to see a negative cash-flow change of 23 percent.

[4] “Global Lighthouse Network: Four durable shifts,” September 2020.

Exhibit 4

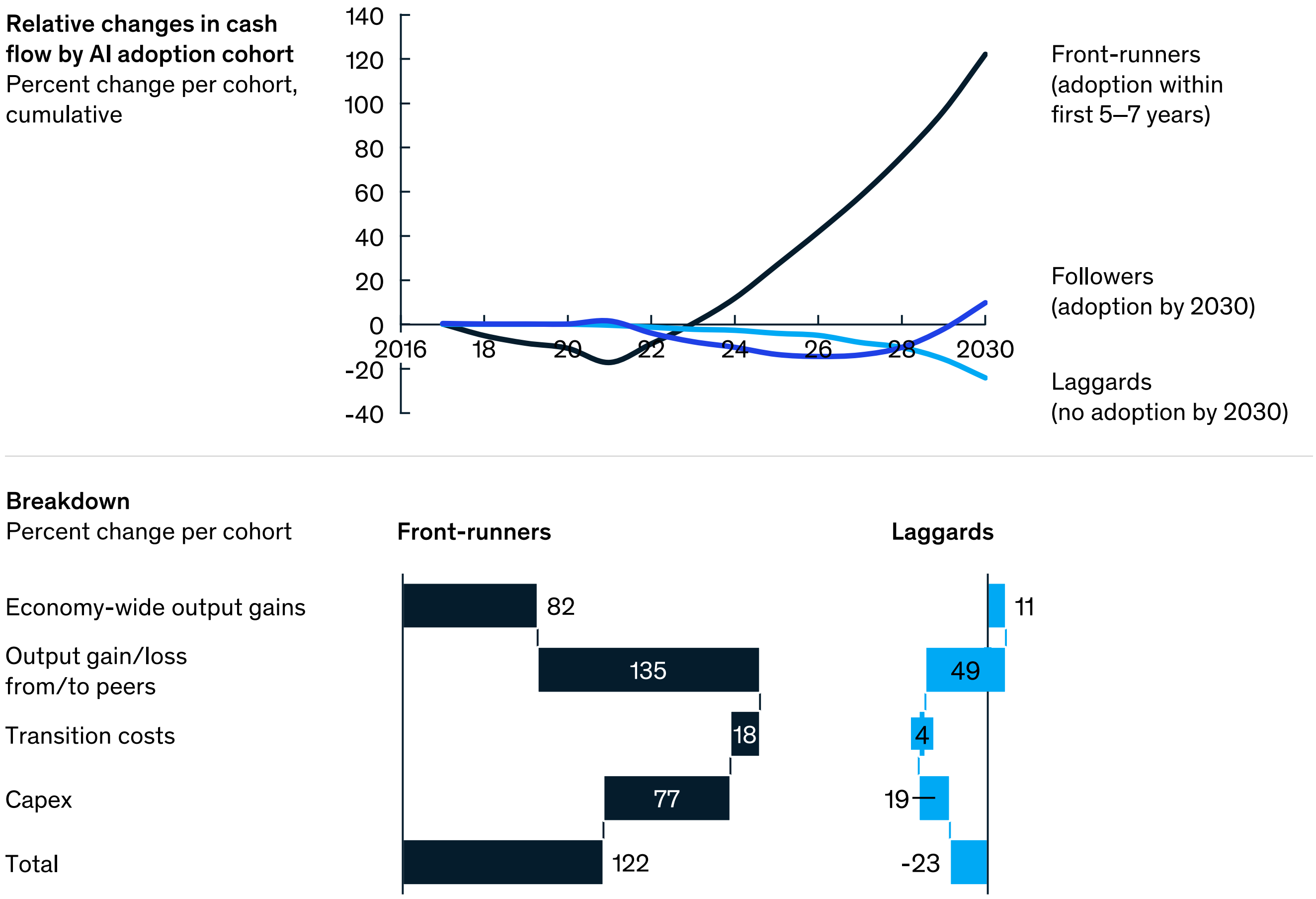
Global lighthouses achieve varying degrees of operational and financial performance improvement—at both the factory and end-to-end levels and across a range of indicators.

Source: World Economic Forum; McKinsey analysis

Exhibit 5

Economic gains by AI front-runners, followers, and laggards show the benefits of early adoption.

Simulation



Note: Numbers are simulated figures to provide directional perspectives rather than a forecast

Source: McKinsey Global Institute

2 Manufacturing companies should continue to commit to digital innovation, and reassess their digital initiatives

As the lighthouse examples demonstrate, IIoT and digital manufacturing solutions can represent important levers for companies to improve their future profitability and competitiveness. What is also becoming clearer is that due to the increasing importance of data and interconnectivity, waiting for less-expensive and better technology will not pay off, as front-runners are expected to capture the largest benefits. Companies, especially those stuck in this “pilot trap,” should swiftly reassess their digital initiatives and define a comprehensive digital transformation program enabling value creation at scale.

To motivate manufacturing companies and act as a guideline, here are six insights into why digital innovation matters, what these companies should take into consideration, and what they should do in this context:

IIoT adoption is real, pays off, and helps manufacturers stay (digitally) relevant
Although we see signs that IIoT adoption has been slower than expected, it is nevertheless real and becoming more widespread (Exhibit 6). With digital manufacturing expected to capture a significant share of the overall IoT market by 2025, it is clear that there are big gains to be made.

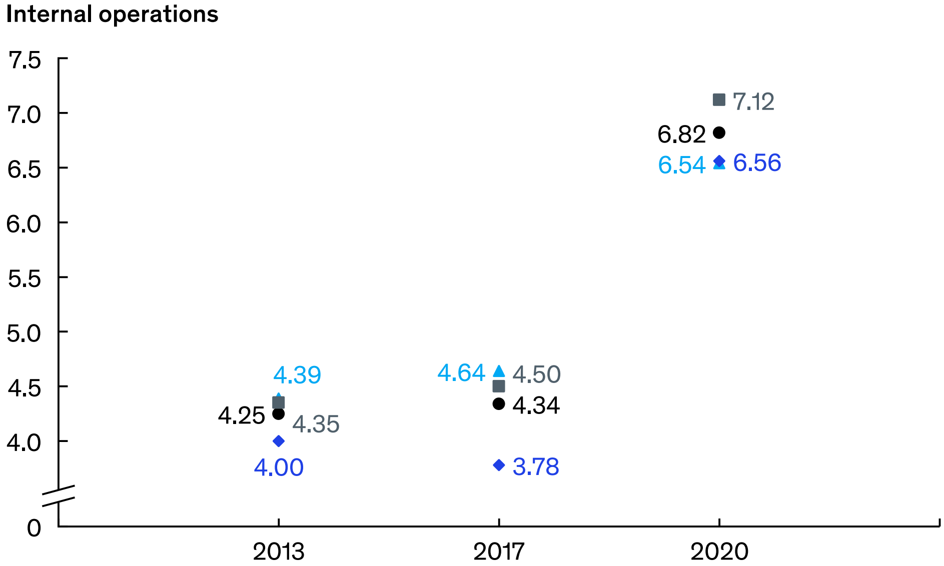
Exhibit 6

IIoT adoption is gaining momentum.

How the IIoT Business Index has progressed
Advances in IIoT adoption from 2013–20

0–2 = nonexistent
2–4 = in research
4–6 = in planning
6–8 = early implementation
8–10 = extensive

- Global
- Europe
- North America
- Asia-Pacific



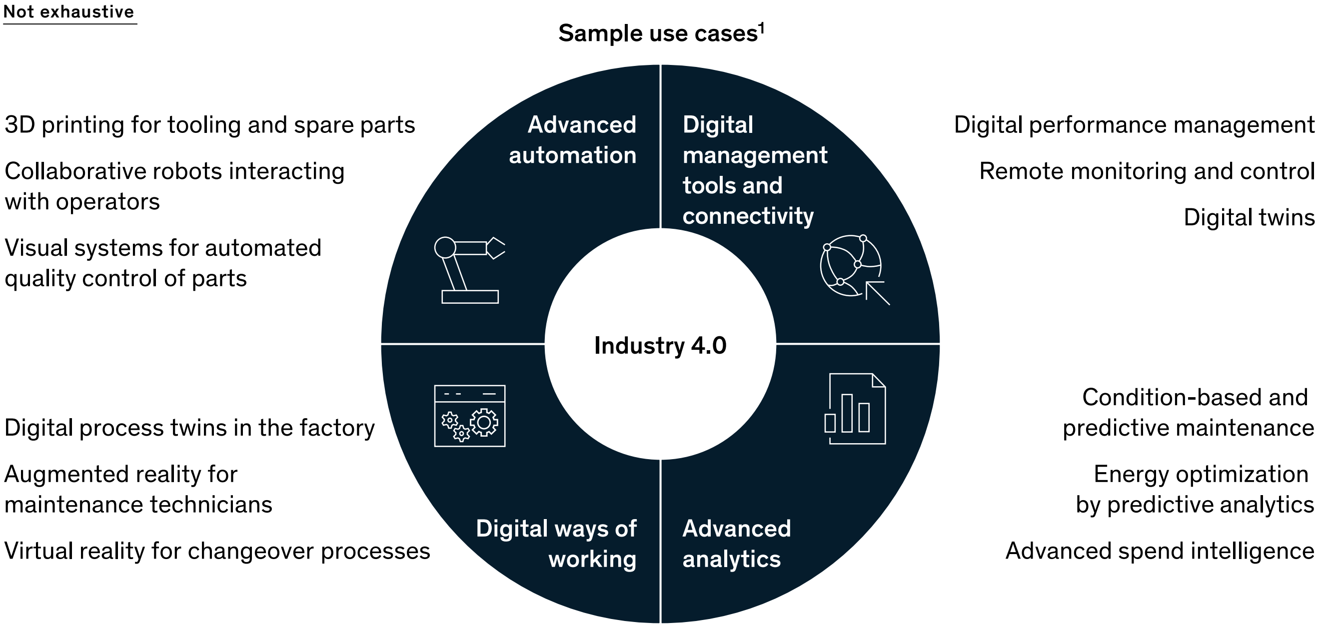
Source: Economist Intelligence Unit

This value, of which a significant share will be attributable to substantial efficiency gains (see Chapter 1.2 and Exhibit 4), is attainable for manufacturers of any size that are willing to commit to digital innovation and leverage core Industry 4.0 technologies that enable numerous use cases available across industries (Exhibit 7).

Exhibit 7

Core Industry 4.0 technologies already enable a multitude of use cases across industries.

Not exhaustive



1. McKinsey's digital use-case library currently comprises 300+ use cases across industries

Source: McKinsey analysis

Besides boosting efficiency and driving innovation, IIoT transformations in manufacturing are also critical because integration and ecosystems require manufacturers to join in and catch up: if one organization carries out an IIoT transformation, all the others have to follow suit to stay relevant and maintain their right to play.[5]

No single application will drive outsize growth, but broad execution is key

Outsize growth will not be driven by any single application; IIoT growth will be driven through a footprint of applications typically yielding $10 million to $100 million in revenue. In other words, no single IIoT use case is a silver bullet at scale, so broad execution (implementing multiple use cases and getting them to scale over time) matters more than picking the optimal use case. The example of the World Economic Forum lighthouses shows which substantial performance improvements in operations are possible in terms of productivity, sustainability, agility, speed to market, and customization.

[5] For further information, see: Agustin Gutierrez, Ashish Kothari, Carolina Mazuera, and Tobias Schoenherr, "Taking supplier collaboration to the next level," McKinsey & Company, July 7, 2020, McKinsey.com.

Shifting toward advanced manufacturing significantly increases manufacturers' resilience

Disruptions such as the one caused by the COVID-19 pandemic demonstrate the importance of continuing and, in some cases, accelerating the ongoing shifts toward advanced manufacturing. This is especially true in the areas of digital planning and management tools and connected and digitized workers:

— **Digital planning and management tools.** The crisis showed that digitized operations can react faster and better to changes, like with end-to-end digital planning tools that enable companies to adjust production capacity early and quickly.

— **Connected and digitized workers.** High levels of digitization contributed to resilience during the early phase of the COVID-19 pandemic because of the increased ability for remote operation.

For manufacturers at the leading edge of IIoT, the pandemic pressure-tested their digital operations in a way not seen before and presented an opportunity to reveal future lessons to be learned.

There are universally relevant key success factors across the dimensions of business, organization, and technology

To escape the "pilot trap" and enable scale, manufacturing companies need to fundamentally reassess their digital initiatives by working across multiple dimensions—business, organization, and technology—simultaneously and with the full commitent of executive management. Just to give an example, although technological barriers (such as plant technical systems, applications, and equipment that do not run on the same operating system) are an important driver of manufacturers' inability to scale their pilot programs, organizational barriers are an even bigger challenge. Table 2 summarizes the key lessons that McKinsey has learned from digital transformations.

The scope and breadth of manufacturing industries represented in the Global Lighthouse Network underscores a key observation—that the key success factors identified in their (specific) manufacturing contexts have a nearly universal relevance.[6]

[6] For further information on the five principles for scaling digital manufacturing, see: Enno de Boer, Søren Fritzen, Rehana Khanam, and Frédéric Lefort, "Preparing for the next normal via digital manufacturing's scaling potential," McKinsey & Company, April 10, 2020, McKinsey.com.

Table 2: Key lessons from digital transformations achieved.

Business	— Digital transformations need to be business-led with a return-on-investment mindset; they are not just another IT project. — An integrated approach across different value-chain steps, including suppliers and customers, delivers the most value. — There is no "silver bullet": impact will come from a broader portfolio of use cases (solutions, applications); but to achieve impact at scale, these need to be organized in domains and prioritized "top down" to address the highest value first.
Organization	— Digital transformations are multiyear, company-wide journeys that need to be driven from the top and require a central transformation engine. — Innovative digital-capability-building approaches allow the rapid upskilling of thousands of employees—besides hiring and retaining the right talent. — Leading companies rapidly shift their way of working by running agile sprints and simultaneously designing and implementing solutions framed by holistic governance fostering the targeted business outcomes.
Technology	— The IIoT infrastructure needs to be radically designed to be future-proof, i.e., scalable across sites and functions, affordable, and secure. — Leading companies build strategic partnerships with key tech players.

While there are companies that are in the lead and can serve as role models, it's still anybody's race

Lighthouses serve as models of successful digital transformations, enabling value creation at scale, and are leading the way by demonstrating how to reimagine and rebalance operations in the next normal of digital manufacturing. However, although they are currently leaders, even lighthouses have not reached the end of their transformation journeys—they are only just starting to unlock the true potential of Industry 4.0 technologies.

In view of this, one thing becomes rather obvious: manufacturing companies should reassess their digital initiatives now. In their efforts to define a comprehensive digital transformation program enabling value creation at scale, they can be expected to benefit from the synthesized "framework for success" that this report introduces and discusses in Part B.

Part B: A framework for success in IIoT-based value capture at scale

Sustainable and scalable digital transformations in discrete and process manufacturing organizations (for information on both industries' relevant similarities and differences in this context, see sidebar, "Similarities and differences between discrete-manufacturing and process-manufacturing organizations regarding sustainable and scalable digital transformations") are ambitious endeavors, strongly focusing on the engagement of the entire organization. Although the implementation of initial use cases can typically be done in around six to eight weeks, a holistic transformation will take two to three years to complete (depending on scope and company size), following three phases and sets of actions (Exhibit 8):

— **Build a baseline and value road map.** Identify the full potential of the business, creating a transformation road map of digital and operational levers, supported by organizational and technology enablers.

— **Mobilize the organization.** Mobilize the organization to develop a detailed transformation plan with bottom-up initiatives fully owned by line leaders.

— **Carry out agile implementation.** Conduct a series of implementation sprints (while continuously refilling the backlog with new items to work off). Launch a full-scale effort to drive value to the bottom line, and scale and institutionalize ways of working.

Similarities and differences between discrete-manufacturing and process-manufacturing organizations regarding sustainable and scalable digital transformations

Overall, it can be said that the process industry and the discrete industry have a very similar reference architecture in the cloud, with variation beginning to emerge in the use of edge devices and becoming stronger the closer it gets to the shop floor. The on-premises differences between discrete and process manufacturers can be described in detail as follows:

Relevant characteristics of the process industry

— **Data availability.** Data availability in the process industry is already advanced because of its historically high degree of sensorization, wiring, and centralization in control rooms, with distributed control systems and supervisory control and data acquisition systems for steering processes and heavy equipment via operators. Hundreds of thousands of variables are available at any moment, and key data is visualized on screens for operators. Both real-time analog values and discrete on/off values are available.

— **Data collection and storage.** In the process industry, all process and machine data is typically recorded in plant historian systems with time stamps. Plant historians serve a function similar to that of a black box on an airplane, allowing forensic analysis in case of incidents. Thus, the process industry has ideal conditions for developing and training algorithms and building AI, given its comprehensive and detailed mass data storage.

Relevant characteristics of the discrete industry

— **Data availability.** In discrete manufacturing, machine-internal sensors are typically hardwired and only produce data to be processed by the machine itself; control rooms rarely exist. Machines are controlled locally via programmable logic controllers (PLCs). If they are interconnected, then only relevant data is exchanged between them. Data is typically not recorded for the long term, unless relevant for quality inspection or tracing production steps. The value of holistic and comprehensive data storage has only recently become understood, and some discrete plants are now adopting a complete data-recording routine. Complications typically arise from machine manufacturers, who consider machine data a trade secret and are unwilling to open up interfaces, although open standards are gradually changing this.

— **Data collection and storage.** Given the lower availability of data in general in discrete manufacturing, data collection and storage proves to be more complicated and is therefore less common. Although awareness of all-encompassing data capture is rising, the actual process of getting the data still depends strongly on the specific use case, in turn creating very specialized data sets. The ability to generate a use-case-independent database that might enable more complex value-adding use cases in the future, such as the optimization of performance across several machines or intelligent interaction between machines, is therefore limited.

That said, irrespective of whether use cases are to be implemented in process or discrete manufacturing organizations, the same seven enabler processes in the areas of business, organization, and technology need to be focused on to create sustainable, feasible, and scalable platforms.

Process industries have already successfully adopted AI-based real-time-optimization models, boosting performance via smarter operation of processes and heavy machinery. For discrete machines, real-time intelligence optimizers have also been piloted at a local level, leading to, for example, energy savings and the increased capacity to adapt to changing conditions by applying machine-learning algorithms in closed-loop mode. Smart applications typically operate on the edge, with interconnectivity via modern communication frameworks with distributed control systems, supervisory control and data acquisition systems, or the PLCs of the local factory machines.

Exhibit 8

Full digital transformations typically take two to three years from initial baseline to profit-and-loss impact.

Activities discussed in Chapters 1.1–3.3

How good can we be?	How do we get there?	Let's make it happen!	
1. Build a baseline and value road maps	**2. Mobilize the organization**	**3. Carry out agile implementation**	**Profit and loss**
Identify the full potential of the business, creating a transformation road map of digital and operational levers, supported by organization and technology enablers	Mobilize the organization to develop a detailed transformation plan, with design initiatives fully owned by line leaders	Conduct a series of implementation sprints (with continual refill to offset leakage) Launch a full-scale effort to drive value to the bottom line; scale and institutionalize ways of working	
Diagnosis: "Size up the prize"	**Design:** "Detail initiatives"	**Monthly transformation sprints:** "Drive impact"	
Duration: ~6–8 weeks	Duration: ~6–10 weeks	Duration: 18–36 months	

Business (Manufacturing)

1.1 Use-case identification and prioritization
- Generate a use-case list
- Set up lighthouse cases for master blueprints
- Catalog, qualify, and prioritize use cases

1.2 Plant rollout and enablement
- Set up value-driven rollout logic
- Start gathering and aggregating data
- Establish the processes for rollout

Organization

2.1 Value capture: Change and performance management
- Define an overall road map
- Implement consistent deviation management
- Set up a value-capture organization

2.2 Capability building and a new way of working
- Identify and fill the skills gap
- Establish structural organizational changes and implement a new way of working
- Manage role transitions and implement a change process

Technology

3.1 IIoT and data infrastructure: Core platform design (incl. IT-OT cybersecurity)
- Fully assess the current factory setup, both in OT and IT
- Create the future target architecture to enable use cases
- Select a partner rather than a vendor to implement the platform
- Effectively manage cybersecurity challenges in IT-OT convergence

3.2 IIoT platform: The cloud imperative in manufacturing
- Make the cloud pay off over the short term
- Tightly manage and control the cloud transformation
- Set up an infrastructure team that can operate much like in app development

3.3 Tech ecosystem
- Understand the key elements of a sustainable ecosystem
- Choose the right partners to achieve balanced partner diversity
- Implement business development to manage the complex ecosystem

Source: McKinsey analysis

To provide pragmatic and actionable insights, this report will focus on seven key enabler processes within these phases in the areas of business, organization, and technology.

From a business perspective, the identification of use cases from a top-down point of view, plus an actionable plan for plant rollout, are paramount for defining goals and the way forward. Once applicable use cases have been identified, an implementation road map that goes hand in hand with the plant rollout plan can be created. Capturing the value of implemented solutions—strongly dependent on newly established ways of working and capabilities—is part of the organizational pillar of the IIoT platform. Within the technology dimension, the required IIoT platform design is developed, making strong use of existing technology offerings along the IIoT technology stack, and the necessary cloud transformation is managed. Additionally, an ecosystem design is created that is focused on the operations and life-cycle management of the IIoT system as a whole.

For various reasons, the temptation may be great to single out individual enabler processes. However, in practice, an overall, holistic digital transformation of the entire manufacturing organization should be the overarching goal. In this way, significantly larger and more sustainable effects can be achieved.

1 Business (Manufacturing)

1.1 Use-case identification and prioritization

This process of identifying and prioritizing use cases (for a definition of this key term, see sidebar, “Definition of a use case”) comprises three steps. The process is also iterative in that if new information arises in one step, previous steps will be revisited, and changes will be made accordingly, like adding new use cases or reprioritizing existing ones.

Definition of a use case

A digital and analytics IIoT use case solves a problem for the user or increases productivity, efficiency, and convenience, mostly with the help of special software. It is differentiated from a normal “ongoing improvement”-type of measure or activity by the following criteria:

— Is significant in size

— Is measurable in terms of impact

— Requires investment and discrete effort

— Requires a decision to move ahead and allocate resources.

Step 1: Generate a comprehensive list of use cases in a combined top-down and bottom-up manner

A comprehensive qualified list of use cases needs to be generated using both top-down and bottom-up approaches.

Top-down/outside-in approach. Use-case libraries hold best-practice case studies and examples from the same or similar industries or functions within the organization.[7] The top-down approach selects potentially suitable use cases from these libraries as a starting point. After an iterative evaluation and selection process, chosen use-case examples will either be directly implemented or used as references.

Bottom-up/inside-out approach. This approach starts with an analysis of existing problems in the actual (physical) processes (bottlenecks, for example). After observing user behaviors via diagnostics and consultative approaches, improvement opportunities are identified. Next, problems can be defined, and ideation exercises can be conducted toward problem resolution. Use cases are then defined and possible solutions are prototyped. Finally, successful use cases are documented, codified, and added to the use-case library for replication.

When using the bottom-up approach, use cases should always be based on operational KPIs that match actual business needs to make sure significant issues are addressed. To devise long-term and more drastic changes instead of incremental ones, a clean-sheet approach should be followed.

Step 2: Catalog, qualify, and prioritize use cases

After an initial comprehensive list of use cases has been generated, the impact and applicability of each use case needs to be analyzed and determined, in order to derive a prioritized subset.

[7] McKinsey’s digital use-case library, for example, currently comprises 300+ use cases across industries.

Impact will usually be quantified in terms of a use case's expected financial impact, that is, exactly how much in incremental cost savings or profit improvement will be achieved by realizing the use case. Then, the use cases can be further prioritized along the lines of ease of implementation. To get there, the total effort and financial investment associated with realizing the use case needs to be estimated, as well as the complexity involved. Finally, the use cases should be mapped on a matrix and clustered according to their ease of implementation and financial impact (Exhibit 9).

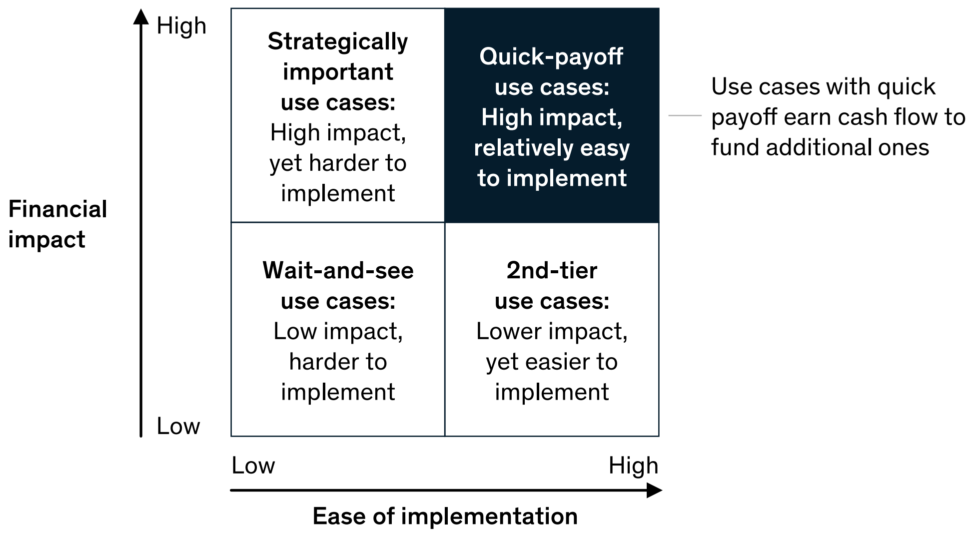
This mapping should provide initial guidance on the relative attractiveness of each use case. Relatively easy-to-implement use cases with high impact should be explored first. The other extreme is use cases that are difficult to implement and, in addition, would only have low financial impact. Not to be dismissed or written off, these use cases belong to the "wait and see" category. Given fast advances in technology, implementation might be much easier two years from now as circumstances change.

Use cases that are more difficult to implement but nevertheless have high impact belong to the "strategically important" category. Enterprises that manage to crack the code as first movers on such use cases may reap the benefits of being first, improving their competitive position. Use cases which are relatively easy to implement but produce low impact may still be carried out, but as second-tier efforts, once the most impactful use cases have been realized.

Once the first prioritizing filter above has been applied, lighthouse cases for initial scalable projects should be identified within the first-priority use cases. Given the technical nature of most cases, hard technical criteria and softer cultural or knowledge criteria will shape the results. An example of such a blended approach is provided in Exhibit 10.

Exhibit 9

Use cases should be prioritized by financial impact and ease of implementation.



Source: McKinsey analysis

Exhibit 10

Evaluation criteria for use cases uses both hard and soft criteria.

Both hard and soft facts will guide the evaluation of use cases in the 1st round

Illustrative

	Indicative selection criteria	Not OK	OK	Good	Ideal	Description of the ideal
Oppor-tunities	**Opportunity size:** How large is the opportunity?				✓	Substantial monetary impact (in line with optimization strategy)
	Data readiness: Do we have enough raw data with sufficient detail?			✓		Readily available, non-fragmented data for key variables for the last year
	Machine condition: Should we plan repairs, maintenance, or longer shut-downs within 1 year?			✓		No major maintenance/down-time during the pilot
Culture	**Innovation experience:** Is there experience in previous technology development projects (e.g., fuzzy logic, big data) and transformation efforts (e.g., maintenance)?			✓		Engineers/operators eager to learn, develop, and innovate Experience with previous digital/innovation projects
	Engineering capacity: Is there spare capacity for an analytics trial on site?			✓		Production engineers, IT/OT/automation managers available
	Lighthouse-effect factor: How visible and impactful will the success of a lighthouse be?				✓	Plant considered a “point of reference” for the organization (in terms of technical compe-tence, experience, etc.)

Source: McKinsey analysis

Step 3: Set up lighthouse cases for master blueprints

At this stage, use cases need to be analyzed in terms of their replication potential across the entire plant network. While some use cases will be unique one-offs, others will be replicable at least once, and some, potentially, multiple times.

In such cases, an overarching lighthouse case is a good start: it serves to solve a particular problem for the first time. The mindset of the team from the outset needs to be focused not only on the technical implementation, but also on investing time in codification, training, tutorials, and other supporting mechanisms, so as to facilitate fast scaling in and rollout to other plants and locations. The initial scalable project will thus require some extra overhead time and effort, but will deliver the reward of fast adoption and replication of the specific use case for other locations and situations throughout the plant network.

1.2 Plant rollout and enablement

We have identified, prioritized, and classified use cases by the number of potential implementations across the entire plant network. The next phase is the development of an implementation road map for use-case adoption. The process comprises the fixed, three-step sequence described below and considers the following criteria:

— Maximum profit impact within a minimum amount of time—local and consolidated

— Available resources and skills as well as employees to be hired and trained

— The logical flow of impact realization, given tax, legal, and other structural constraints

— Market pressures and available investment in support and technology

— The pace of deployment of enabling technology, such as data lakes, sensors, and IIoT platforms

The implementation road map will likely have a longer-term horizon of three years, with more focus on the first 12 to 18 months. The road map defines the "what"—which use cases will be realized, the "how"—how they will be realized, and the "who"—who will be responsible for realizing them. A master plan with concrete actions, deliverables, timelines, and realization steps will track all measures precisely and provide updates for monitoring and correction purposes.

Step 1: Set up a rollout that is value driven and pursues impact

Rolling out the first use cases is an investment, and it is therefore important to think about the rollout in a strategic way (see the automotive example in Exhibit 11). In most situations, it is recommended to roll out the use cases based on value/feasibility. First, choose the use cases that create immediate value, and avoid the use cases that require databases that must be built from scratch or other high-effort prerequisites. While the focus is usually on low-effort, high-value use cases, there are strong arguments for pursuing use cases with low or no return on investment. For example, a use case may not lead to immediate value but it may enable future use cases. This decision is analyzed up front, and the justification needs to be clearly communicated so that all relevant stakeholders are aware of the investment and the value, even if that value is delayed.

Proven best practices for successful use-case rollout are:

— **Work agilely.** The rollout approach should be an agile one. Define rollout waves and align the waves with the teams. Be flexible and adjust future waves if needed, but avoid making adjustments to the current wave—this leads to unnecessary "noise" and slows down the overall rollout.

— **Maintain standards and enable learning.** It's always good to roll out use cases in plants with a slight time offset, irrespective of whether the plant network is heterogeneous or homogeneous. This ensures that lessons from a rollout at one plant can be applied to subsequent rollouts at other plants. Ensure a stable feedback process to alert rollout teams of upcoming problems, and ensure an exchange of running code (on site if necessary; the cloud back end should be the same) to leverage knowledge and avoid duplication of effort.

Exhibit 11

Achieving impact at scale requires a clear, phased rollout approach over multiple waves.

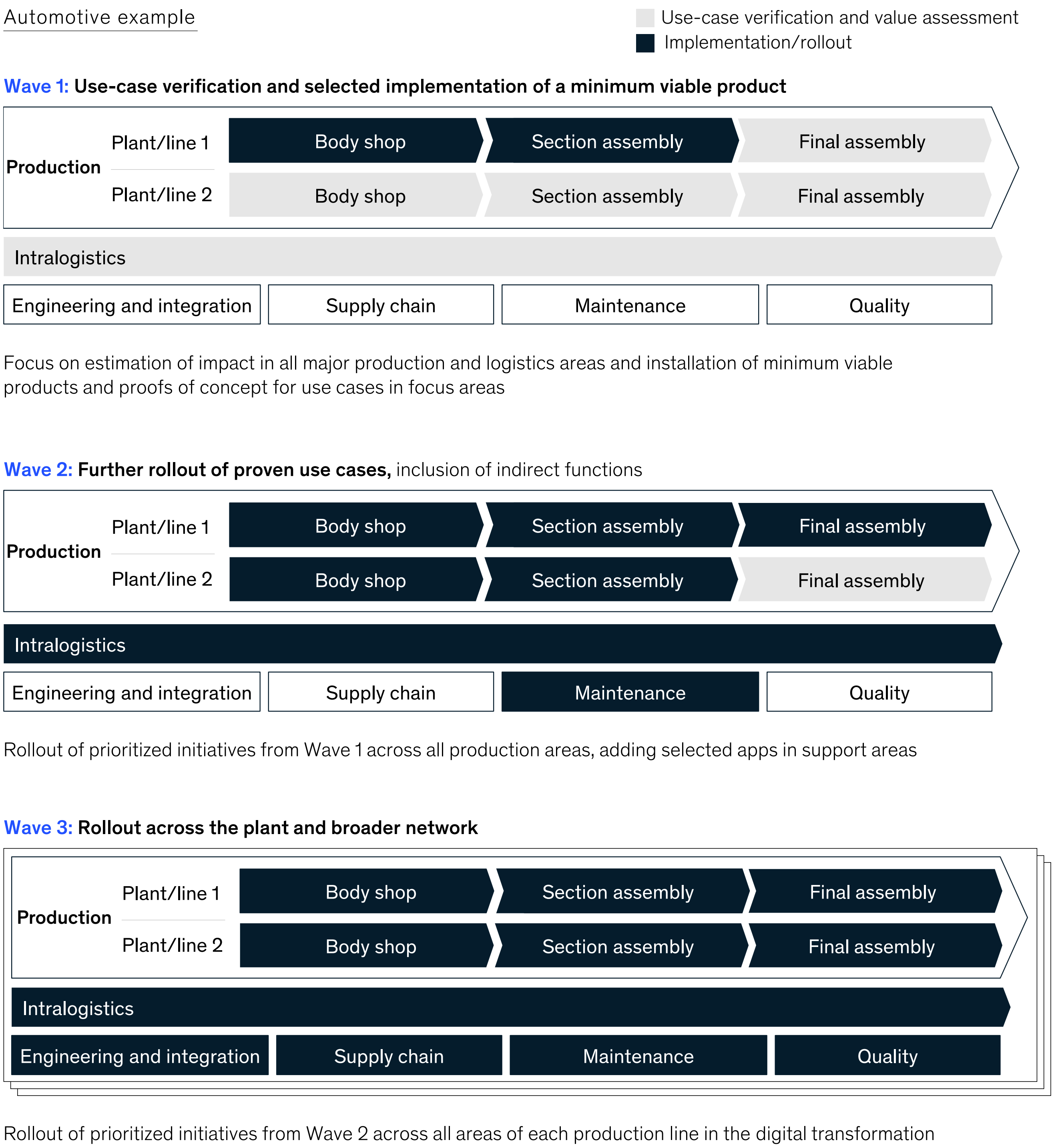


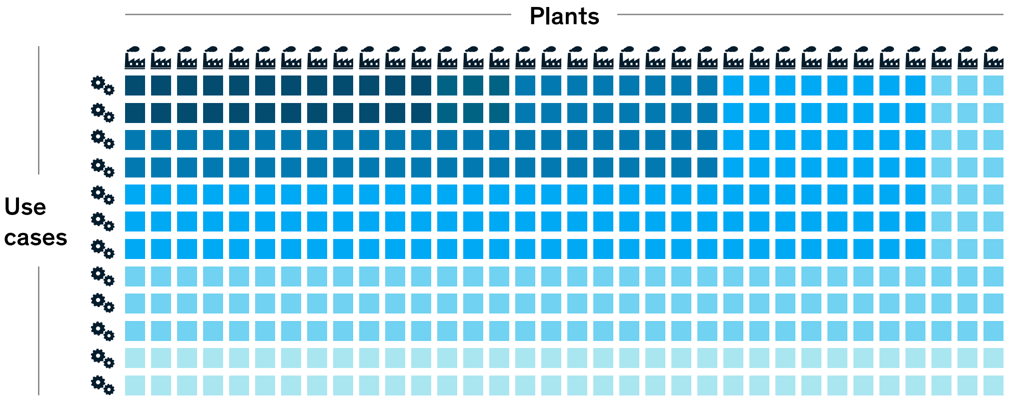
Exhibit 12 provides an overview of a use-case rollout over a large number of factory sites. This particular rollout was for a company that could implement the same use cases in different locations due to the similarity of its lines and products.

If the plant network is heterogeneous (different lines, products, and industries), a differentiated case-by-case rollout plan is recommended, always keeping in mind the best approach for clustering efforts. By using a value-driven approach, it's easy to identify a first cluster, which can still be refined during rollout, to start the implementation quickly.

The only layer that might look different in each plant is the machine/edge connectivity and data collection. As a consequence of different types of machines with different hardware (running different protocols) hailing from different periods in time, this layer is the most heterogeneous one from a historical point of view and thus needs specific, well-clustered solutions. There will eventually be more clusters; however, using the same hardware/software for connecting specific types of data sources (for example, types of PLC brands) will help to make future maintenance easier by keeping the number of different systems as low as possible.

Exhibit 12

Rollout should start with a few use cases at several plants.



Key advantages

Scalability of use-case implementation is secured from the start

Complexity of connecting heterogenous plants is tackled from the start

Siloed, plant-specific solutions are prevented

1 **Ramp-up phase:** Connect multiple complex and heterogeneous plants and implement first use cases

2 **3** **4** **Continuous rollout with steady capacity:** Connect multiple plants in each wave and implement more use cases

5 **Final phase:** Implement remaining use cases across all plants

Source: McKinsey analysis

Step 2: Start gathering and aggregating data, conducting important activities in parallel

Not all of the pieces need to be firmly in place before the rollout begins. Specifically, even before the requisite data is connected, use-case prioritization provides an overview of the necessary data sources and an understanding of what data is available and connectable. Based on this information, the architecture for data gathering can be adjusted or defined for the specific OT hardware and data-source situation.

In parallel, however, platform core development should not be neglected and should begin in synchronization with use-case development. The sources need to be connected for automated data collection as soon as possible. Depending on the status of implementation of the target architecture, the use case can be deployed on an on-premises server, based on the defined architecture. This involves the use of frameworks, which will ultimately be used in the back end. But it shouldn't take long to implement the final architecture with prioritization of the first use cases, and migration of the first use cases should be possible after just a few weeks. Going forward, every use case is implemented in the target architecture. In preparation for this, the next wave of use cases should be looked at and enabled by being connected to the necessary data sources in the earlier wave(s).

What needs to be considered here is that many use cases need more preparation time, simply due to the fact that some data sources do not yet exist. To make up for this, it may be necessary to add sensors, change machines' PLC logic, update systems, and so on.

Step 3: Establish the processes and collaboration that enable the required rollout

A standard onboarding process for new plants must be established to ensure that a team is in place when the rollout starts there. A rollout is also a transformation of an organization's way of working and mindset; thus, it is important to make mindful change management as much of a priority as the rollout itself. The success of a use case can be undermined if the benefit has not been made clear and the people either fail to use the new application or system in their daily work or use it incorrectly.

A central IIoT rollout team takes care of the needs at different plants by ensuring that everything is in place before the rollout starts. The list of needs includes both the skills and the technical foundation that the use case requires. The central IIoT team identifies the right people on site to manage the rollout and also contributes knowledge toward problem solving, as questions might arise due to unknown site specifics. The central team also tracks the status of the rollout and the problems that occur. This ensures a holistic view of the benefits, implementation status, and solutions to problems to derive best practices for the next plants. A deeper look into the use cases will almost certainly reveal the need for skills that might not currently exist within the organization or individual plants. Onboarding of new talent or training of current employees must begin early so that the skills are in place when they are needed. Skill development and capability building are continuous endeavors because the rollout of use cases is never-ending. Investment in these areas is mandatory for an organization that wants to be successful in its Industry 4.0 efforts.

It is also key to have a clear collaboration model in which there is one person defined per workstream with clear accountability. Effective communication within the organization, such as cross-plant communication, and between the organization and its partners must be ensured. Important partner archetypes along the value chain are industrial equipment providers, technology providers and integrators, and functional domain specialists.

Employee training must begin in advance of the rollout (or even simultaneously), so that they are aware of and believe in the new opportunities and can benefit from the use case. Learning sessions are critical, with time invested for answering employee questions and concerns. Additionally, involving the people who will work with the new application or tool in the development process and soliciting their feedback can have the effect of not only creating a tool that better fits their needs but also of increasing acceptance of, buy-in for, and, ultimately, use of the new application or system. It will also be important to establish expectations and responsibilities of use-case owners, as they will define subsequent sprints within the use cases and report status updates as well as problems. Alignment on processes, such as how communication happens and how status and progress are measured, is important.

In addition to the road map, there must be a clear understanding of the starting position in technical terms—by understanding the current IT and OT landscape (see Chapter 3.1)—but also in organizational terms.

2 Organization

While it may be tempting to underestimate this supposedly "soft factor," companies should be aware that they cannot take the organizational dimension seriously enough. Overcoming organizational barriers is a precondition to successfully managing the technological part of a digital transformation in manufacturing. Accordingly, the two enablers for capturing value, establishing a new way of working and building capabilities, will be discussed in the following.

2.1 Value capture: Change and performance management

The value of a digital transformation in manufacturing is tied to the sustainable implementation of use cases. Thus, capturing the value of those use cases is essential for successfully steering the IIoT transformation. This requires the organization to set clear target values along a road map of the entire transformation and have streamlined tracking and reporting as well as strong deviation management in place. Holistic tracking of the implementation across all plants is mandatory for further rollout and prioritization of use cases for implementation (next-wave planning).

Step 1: Define an overall road map of the IIoT transformation and use-case target values

The most important cornerstones of a structured approach to value capture in a digital transformation are to have a stringent road map with major milestones for projects and use cases in place and to set target values for those use cases along the road map. Besides the estimated impact value of a use case, those target values should also include KPIs for the budget and an overall status along the timeline. The impact estimation may also be used for the prioritization, completion of implementation, and rollout planning of use cases.

To get a full and accurate measure of the value capture of IIoT-enabled advanced technologies, it is important to take a holistic view of the use cases along the road map. This means understanding the entire implementation process, starting with the selection of the use case, moving through the improvement cycles, and finally, looking at scaling and industrialization.

Step 2: Set up a value-capture organization, model, and mechanism

To execute on value capture of a digital transformation in manufacturing, a dedicated value-capture organization is recommended. A value-capture office may act as a central unit for coordinating the reporting and communication of the overall state of the implementation to the management board and other stakeholders. To be able to monitor the use cases' value effect toward defined target values, (ideally automated) tracking and reporting is needed. To avoid version conflicts and enable speed and currency of data, a central database acting as a single source of truth is key. Reports should be tailored to the different hierarchy levels involved in steering the program. This includes the aggregation of cost and value figures for distinct hierarchy levels.

Beyond simple reporting, the value-capture office is also charged with monitoring the achievement of target values and intervening if the value captured is off target. The value-capture office may therefore deploy and steer task forces (such as from a central pool of experts) to support implementation of use cases (in plants, for example).

Step 3: Implement consistent deviation management

The value-capture office needs to take the lead in implementing strong deviation management. This enables it to:

a) Identify deviations from the implementation plan and investigate underlying reasons, including overarching challenges and bottlenecks in the overall program beyond individual use cases.

b) Define mitigation measures to bring use-case development and implementation back on track.

c) Support the implementation of measures by use-case/project leads, for example, by deploying task forces.

2.2 Capability building and a new way of working

A digital transformation in manufacturing goes hand in hand with massive organizational changes. This includes changes to organizational structures, collaboration partners and types, and job profiles and roles. As a result, a new way of working and a new set of capabilities are required to successfully implement and scale IIoT and digitally enabled use cases. The following actions are crucial for a successful transformation. We have defined them here as "steps," but whether they are implemented sequentially or concurrently will depend on the specifics of the organization, including its particular starting point.

Step 1: Establish structural organizational changes and implement new governance and a new way of working

A holistic digital transformation in manufacturing requires the involvement of several functions and entities (plant organization, IT, OT, and central production entities, for example) and thus results in new functional interfaces and the need for a cross-functional way of working. This requires breaking down rigid organizational boundaries, which are often deeply rooted in large organizations. When aiming for IT-OT convergence, organizations typically face several challenges (Exhibit 13):

— Complex decision making due to split responsibilities between IT and OT, especially regarding cybersecurity

— Lack of joint governance bodies and structures to align IT and OT interests and needs

— Slow adoption of new technologies in OT environments—for example, cloud, continuous integration, and continuous delivery

— Limited joint management and execution of cross-technology (IT and OT) strategies and projects

— Lack of standardization and process harmonization across plants

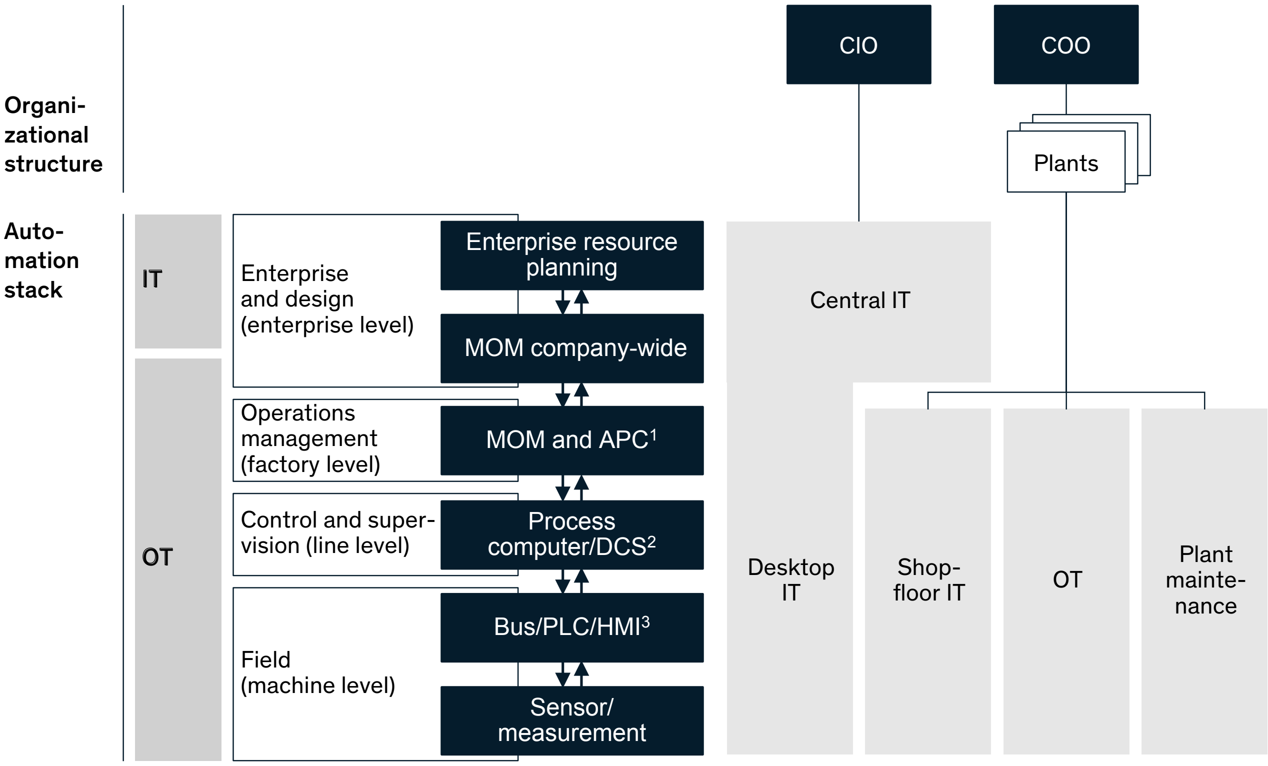
— High degree of duplicate or overlapping processes between IT and OT

— Lack of interdisciplinary skill profiles covering both IT and OT requirements

Also, the integration of external entities as new collaboration partners with different organizational setups and ways of working calls for a new organizational setup for the manufacturer. To coordinate use-case development in the plants, a central team of experts with cross-functional skill profiles covering both IT and OT requirements can, in conjunction with the IT department, support development efforts, provide technical expertise, and help with the technical deployment of, for example, cloud-based IIoT technology in the form of an IIoT platform. This team sets standards and provides best practices to the decentralized plant organization and incorporates the plants' requirements to support the rollout of an IIoT platform and use cases (Exhibit 14). This central team can also be leveraged by the value-capture office to deploy task forces in cases of delays in implementation.

Exhibit 13

IT and OT are typically managed by different functions, hindering IIoT enablement and adoption.



Observations

IT and OT are often managed independently and treated as isolated technologies, as their convergence has not been foreseen by most companies

While IT is managed by the CIO, OT systems are managed by the COO or business unit manager

Hence, IT and OT implementations cater to different problems and employ different architectures and protocols

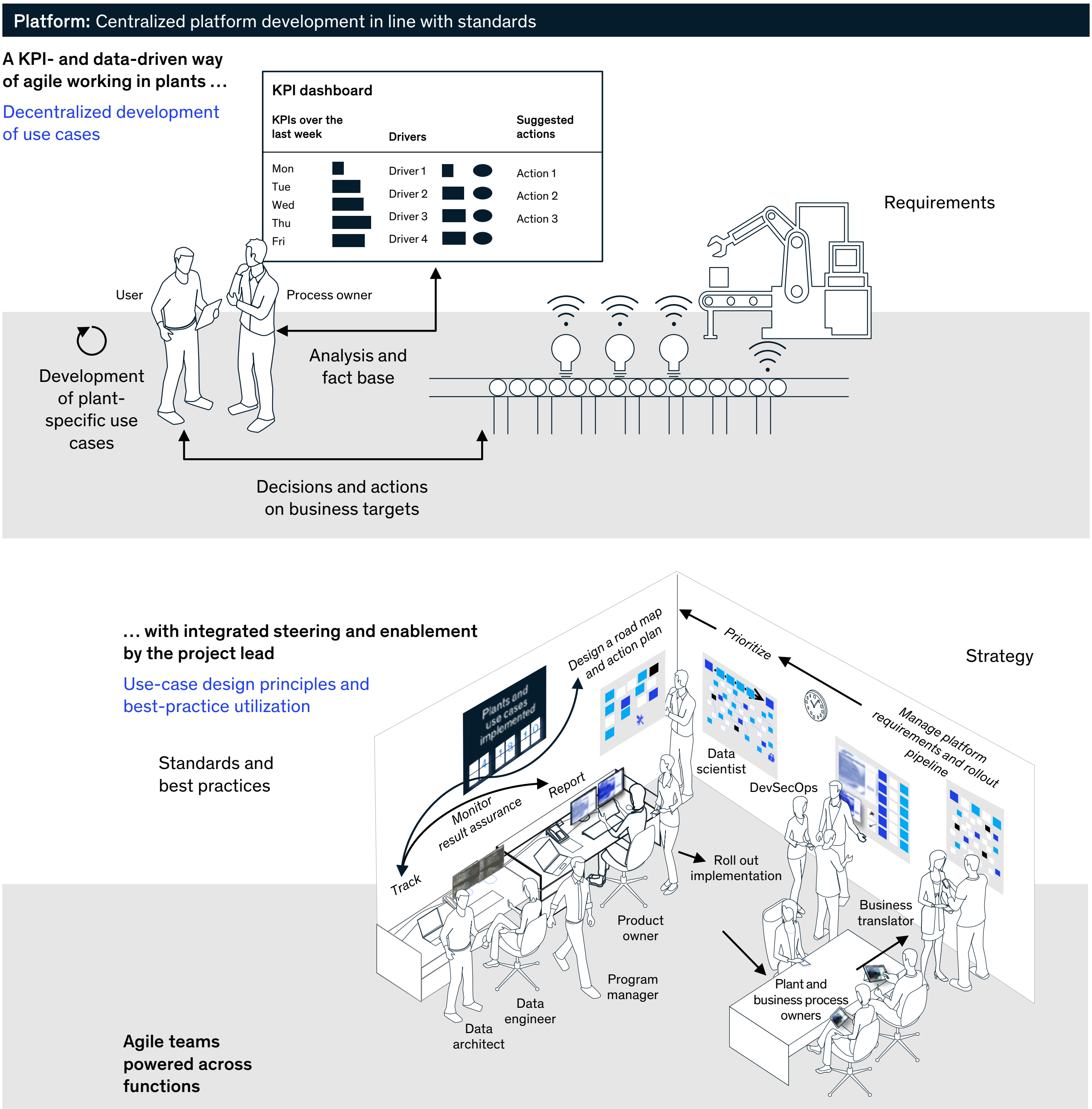
This results in inefficient, costly setups that only enable a low degree of innovation and standardization

1. Advanced process control
2. Distributed control system
3. Human–machine interface

Source: McKinsey analysis

Exhibit 14

Digital production technology will enable a new way of working, with a central project lead steering and supporting platform and use-case rollout across plants.



Source: McKinsey analysis

There is certainly no single, standardized approach to establishing a converged IT-OT organization. This report's findings concerning this challenge, as well as McKinsey's observations of the most successful players that have adopted this type of organization, however, reveal the following guiding principles for converging IT and OT:

— **Common governance model**

  - Establish central governance bodies incorporating both IT and OT expertise to define guiding principles for IT and OT in the future.
  - Define a common architecture model for both IT and OT based on industry standards.

— **Process harmonization**

  - Harmonize duplicate and overlapping processes across IT and OT based on the overarching guiding principles and an integrated organizational model.
  - Standardize processes across plants to enable improved quality management.

— **Common KPIs**

  - Implement a common set of KPIs (measuring implementation processes and value capture) for both IT and OT to incentivize IT-OT convergence.
  - Ensure fast and continuous implementation of new products, technologies, and features into manufacturing processes to reduce cost and time to market.

— **Central data and security management**

  - Formalize governance and security policies for OT.
  - Establish single-point accountability for OT and IT security.
  - Leverage an integrated approach to security and incident management across IT and OT to facilitate enhanced security measures against external threats and central security governance along the entire value chain.

— **Skills transformation**

  - Define roles and skill profiles that support the integrated operating model and governance.
  - Define the reskilling approach for existing resources and derive a long-term hiring plan.

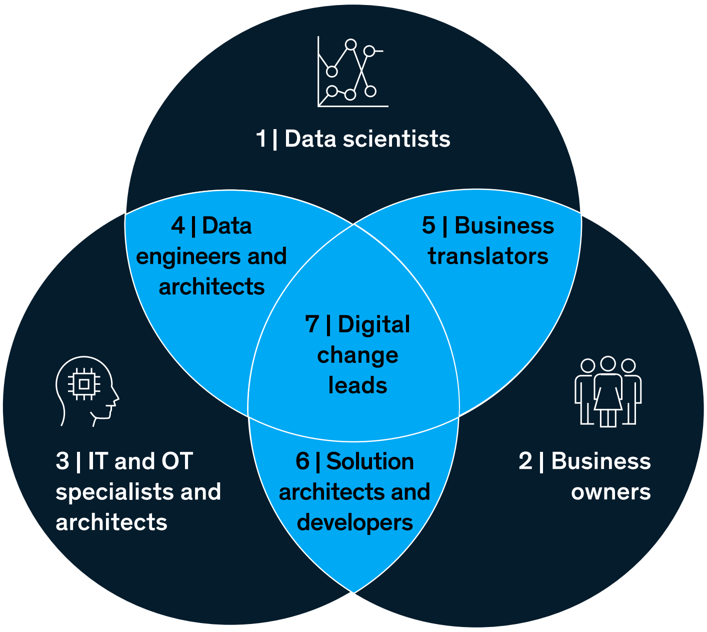
Step 2: Identify and fill the skills gap

To achieve sustainable value from a digital transformation in manufacturing, job profiles, especially in plants, will shift toward IIoT and digital capabilities for direct and indirect personnel. Hence, the required roles and capabilities of the future organization need to be defined. Specifically, the right skills need to be in place for the development, deployment, and operation of digital use cases. Data scientists, IT and OT experts, and business owners need to work hand in hand, and also call for new roles to be established (Exhibit 15).

Data engineers, business translators, and solution architects embody just some of the new roles that are needed (Exhibit 16) but do not typically exist in nondigital manufacturing organizations. Next to external hiring, a great source of new skills can be found in the existing employee

Exhibit 15

A new people paradigm sits at the interface between traditional functions.



Role description

1 Create data structures suitable for analysis and run advanced analytics models to generate insights and predict future events

2 Provide business input as functional users to develop and later own use cases

3 Manage the technical aspects of automation projects and the technology landscape

4 Manage data infrastructure, ensuring robustness of pipelines and building features; clean and structure data

5 Identify digital opportunities and facilitate the interface between business and data scientists in iterating models and insights

6 Develop the solution architecture and user interface

7 Coordinate resources and requirements to deliver business impact

Source: McKinsey analysis

pool through reallocating resources, and training and reskilling the existing workforce. Many required, future roles will be an evolution of skills that typically already exist, like use-case-driven process changes that will be implemented by process engineers, or OT connectivity and retrofitting, which will become new elements of maintenance or automation technicians roles.

Exhibit 16 shows an example of synergies between old and new roles. Focused training for employees of different divisions is mandatory. This requires careful consideration of the (often vastly) different levels and types of knowledge. A “ramp-up” component of the training can help get everyone to a minimum knowledge baseline before beginning the more focused part of the training.

Step 3: Manage role transitions and implement a change process to support a mindset shift across hierarchy levels

Transforming the workforce toward the new skill set required in the future needs careful management of role transitions. This process includes a definition of all necessary skills and the design of development paths, including the transition from “old” roles to “new” roles. The development paths should be defined in detail and made fully transparent to all staff. A clear perspective on personal and professional development and requirements for the future helps engender trust in and buy-in for the new technology among the workforce. In order for

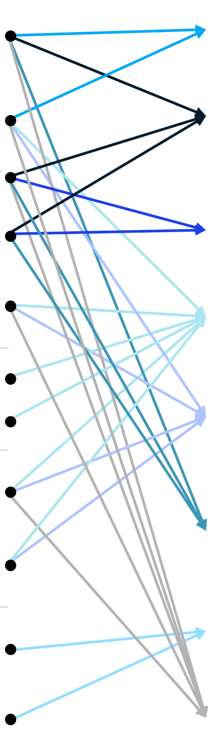
Exhibit 16

New roles can be partially filled with existing employees after coordinated reskilling.

Example

Possibility to staff new roles from in-house resources: Easy | Medium | Difficult

	Classic roles
Engineering and IT	Process and automation engineering
	Logistics coordination
	Plant IT
	Plant network IT
	Quality engineering
Plant logistics and quality	Plant logistics
	Quality
Production coordination and planning	Production coordination
	Production planning
Production operations and maintenance	Maintenance – mechanical
	Maintenance – electrical



New roles	Responsibilities	Typical in-house availability at tech and AI players
A | Data engineer and architect	Manages data infrastructure; cleans and structures data	Intensive reskilling of some employees; complemented by external hires
B | Data scientist	Creates and cleans data structures suitable for analysis; runs models to generate insights	Several employees can be upskilled, but additional hiring might be required
C | Data security officer	Provides a safe environment for data	Several employees can be upskilled, but additional hiring might be required
D | Business translator	Identifies digital opportunities, facilitates the interface between business and data scientists	Technical employees can easily be trained to become practitioners
E | UX/UI designer	Develops the user experience; ensures user interfaces support business activity	Some expert hires might be required
F | Solution architect and developer	Develops the solution architecture and user interface	Technical employees can be trained with some effort
G | Systems maintenance technician	Identifies digital opportunities; provides support/expertise to the digital transformation team	Intensive reskilling of some employees; complemented by external hires
H | IT-OT integrator	Enables data exchange from hardware items	Technical employees can be upskilled through insights on hardware connectivity

Source: McKinsey analysis

the whole workforce to capture the full potential of IIoT, a change management process is necessary to develop and distribute the new skills.

For organizations embarking on a digital transformation in manufacturing, it is paramount to acknowledge that the skills transformation of the workforce is not a "by-product." It affects the whole organization at its core, with up to 90 percent of the workforce (in particular in the plants) impacted by training, reskilling, or the hiring of external talent (Exhibit 17).

Building the right skills within the organization and setting up the workforce for the future is a core success factor in achieving sustainable business impact. Especially for large organizations, a well-designed and well-executed workforce transition will also be critical for organizational health. Aspects of this transition include employee motivation and satisfaction and the safeguarding of knowledge and skills. Both business impact and organizational health are mission-critical for a successful digital transformation in manufacturing.

Exhibit 17

The plant of the future may achieve the required workforce by training, reskilling, and hiring.

Example

10–25%

No action required

Skills are already in place since roles do not undergo big changes ; this is mostly applicable for management and coordination roles

50–65%

Training

Skills and capabilities for the new tasks in existing roles can be developed internally through an end-to-end learning journey; this is an important strategy for roles across the entire plant

10–15%

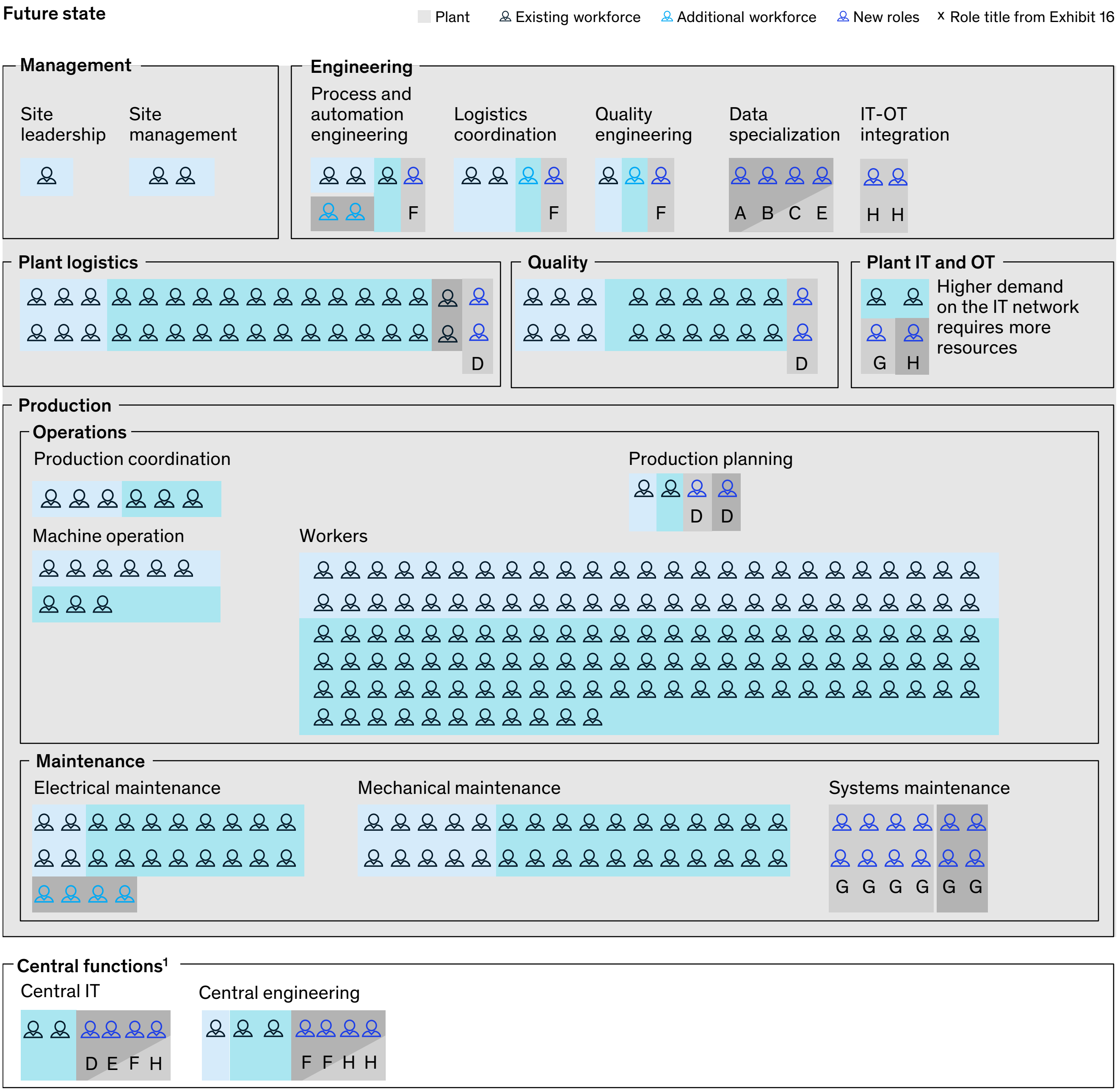
Reskilling

Skills and capabilities for new roles can be developed internally through the identification and reskilling of potential talent in the internal workforce; new roles in IT, engineering, and maintenance can be filled internally using this approach

15–20%

Hiring

Skills cannot be developed internally through training and reskilling and have to be found externally through hiring; this is significant for digital roles with a strong IT link



1. Dual reporting line from internal plant roles to central IT in order to avoid isolated development of solutions in separate business units

Source: McKinse analysis

3 Technology

After making the business case for industrial stack development—and the use cases it enables—the next focus is on technology at the three levels of data infrastructure, cloud integration, and ecosystem.

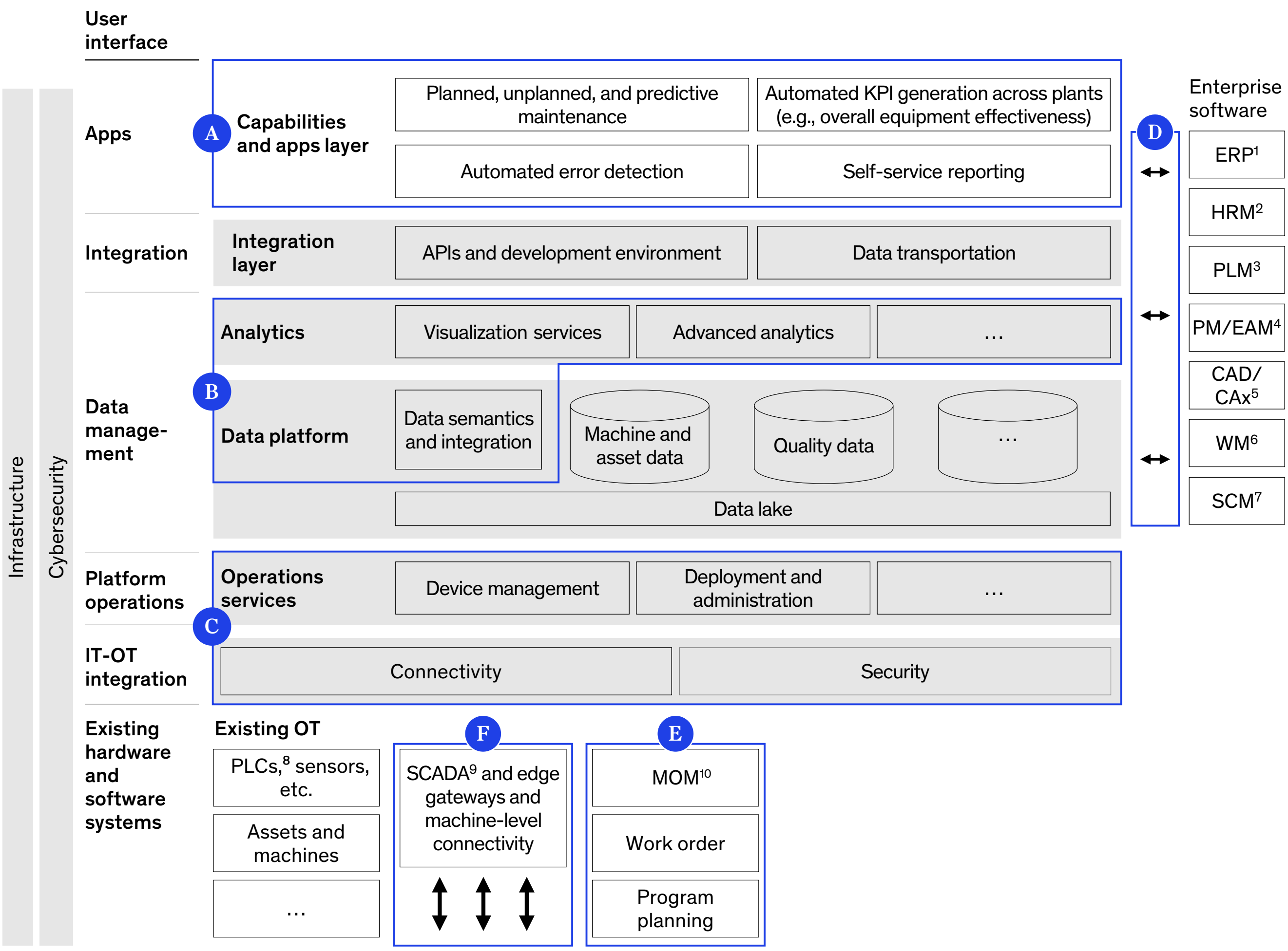
3.1 IIoT and data infrastructure: Core platform design (including IT-OT cybersecurity)

The core platform design is focused primarily on creating the future target architecture of the IIoT platform (see sidebar, "What is a platform?"). The future target architecture covers all relevant technical requirements of the identified use cases based on captured data and decision flows in the IIoT platform within the context of the brownfield manufacturing environment (Exhibits 18 and 19).

Exhibit 18

A manufacturing company's target architecture integrates ERP, MOM, PLM, and IIoT into one platform.

Example: IIoT platform in production and logistics   Illustrative   Key functions and value add of IIoT platform   IIoT platform elements



1. Enterprise resource planning
2. Human resources management
3. Product life-cycle management
4. Plant maintenance / enterprise asset management
5. Computer-aided design/technology
6. Warehouse management
7. Supply-chain management
8. Programmable logic controller
9. Supervisory control and data acquisition
10. Manufacturing operations management

Source: McKinsey analysis

Exhibit 19

Several key aspects need to be detailed to be considered in the target architecture and the implementation road map.

Key function (from Exhibit 18)

A

Capabilities and apps layer

Apps covering specific use cases, e.g., predictive maintenance or automated error detection, that build upon standardized platform functionality

Apps provided by a third party or platform provider and available via an app store, e.g., overall equipment effectiveness for machines

B

Analytics and data platform

Standardized (self-service) reporting, analytics, visualization, or location services available via API to all apps utilizing best-in-class algorithm libraries

Integration and harmonization of data, taking semantics of different protocols and machines into account

C

Operations services

Highly scalable services handling basic platform functionalities such as device management (e.g., rights and roles, access management), service hosting, deployment and administration (e.g., activity monitoring, resource use), connectivity, and security (e.g., encrypted data exchange, key public infrastructure, certificates) available to all sites based on microservices and API

D

Integration into enterprise IT systems

Interface to enterprise-level software, e.g., ERP, SCM, PLM, or CAD, via aggregating data and information generated in the app or analytics and data platform layers in formats processable by enterprise-level software

Enterprise-level software with access to the analytics and data platform and potentially also apps via API to perform processing that is not natively available

E

Integration of the IIoT platform with MOM

Integration of the IIoT platform with the MOM layer to enable detailed scheduling of production, shifts, orders, and overall lines, and configuration and status information—input for operations analytics (quality, asset maintenance, overall equipment effectiveness) and other custom apps

F

SCADA, edge gateways, and machine-level connectivity

Data routing and exchange with edge devices and machines, incl. data flow prioritization engines for forwarding raw or preprocessed data to the cloud

Data routing, prioritization, and storage enabled by on-site processing and storage within edge gateways

Easy integration of devices into the platform via plug and play

Source: McKinsey analysis

As a prerequisite, core platform design therefore requires: a) understanding which advances in industrial automation and IT-OT integration IIoT platform technology offers and why, and b) beginning with well-defined, prioritized use cases (Exhibit 20).

What is a platform?

The term "platform" is overused to the point where it does not convey much information beyond "more assembly required." Most broadly, a platform is software and hardware, which may include an operating environment, storage, computing power, security, development tools, and many other common functions.

Platforms are helpful because they abstract a lot of common functions away from the specific application logic. Application developers just want to focus on the specific problem they are solving and use common capabilities for computing power, storage, or security. A good platform thus dramatically reduces the cost of developing and maintaining applications.

Exhibit 20

Demystifying the platform—the sum of enabling technologies to support apps and analytics.

Platform
Can be hosted on-premises, as a company-internal service, or by a 3rd party

Layer		IIoT automation stack	Tech stack		Stack components						
Enterprise and design (firm level, incl. suppliers)	*Cloud*	Cloud apps	Software infrastructure and apps	Apps	Enterprise and consumer apps	App store	Self-service portal/UI				
Enterprise and design (firm level, incl. suppliers)	*Cloud*	Cloud apps	Software infrastructure and apps	Apps	Analytics and visualization	Data orchestration	Machine learning	Rules engine			
Enterprise and design (firm level, incl. suppliers)	*Cloud*	IoT/cloud platform	Software infrastructure and apps	Cloud infrastructure	Data processing	Protocol normalization	Data caching/storing	Data validation	Data logging	Apache Hadoop	
Enterprise and design (firm level, incl. suppliers)	*Cloud*	IoT/cloud platform	Software infrastructure and apps	Cloud infrastructure	Data storage	Relational database	Non-relational database	Operational data stores	Data backup and warehouse	Data indexing	Orchestration and security
Operations mgmt (factory level)	*On-premises software*	Apps	Software infrastructure and apps	Enablement platform	API management	API publishing and discovery	Tokenization/authentication	API analytics/reporting	Developer tools/portal		
Operations mgmt (factory level)	*On-premises software*	System solutions	Software infrastructure and apps	Enablement platform	App engine	Software development kit	Search and query	User authentication	Blob management	Algorithms engine	
Operations mgmt (factory level)	*On-premises software*	System solutions	Software infrastructure and apps	Enablement platform	Device management	Registration and password mgmt	Policy mgmt and key rotation	Authentication	Log tracking	Configuration mgmt	Patching/updates
Operations mgmt (factory level)	*On-premises software*	Connectivity	Connectivity		Backhaul	2G/3G/4G/LTE/5G	LTE-U	Wired			
Control and supervision (line level)	*Embedded*	Connectivity	Connectivity		Local	Wi-Fi	BT broadband	Near-field communication	802.15.4 (Zigbee)	Infrared	DSRC
Control and supervision (line level)	*Embedded*	Security	Security		Endpoint protection and IAM	Threat detection	Identity and access mgmt	Antivirus			
Control and supervision (line level)	*Embedded*	Embedded software	Hardware (and embedded software)		Devices/packaging						
Field (machine level)		Smart sensors	Hardware (and embedded software)		On-device software	Software development kit[1]	Hardware development kit	Real-time operating system	Firmware, drivers	Operating system	API
Field (machine level)		Machines/hardware	Hardware (and embedded software)		Board-level components	Processors	Analog front-end sensors	Modems	Secure boot loader	Data caching/storing	Actuators

1. Incl. message bus

Source: McKinsey analysis

IIoT platform technology offers advances in industrial automation and IT-OT integration

For decades, the world's many industries have invested heavily in IT to reduce costs, improve operational efficiency and visibility, and, ultimately, to boost profits. In doing so, IT professionals have laid the foundation for what is called the digital enterprise, meaning an organization that uses technology as a competitive advantage in its internal and external operations. Yet while IT used to be mostly about back offices—finance, accounting, HR, or office productivity—a ("fully") digital enterprise nowadays also leverages IT and connected devices in the very place where the company actually creates value for customers, such as, for industrial companies, in manufacturing, design, and service. Thus, for the extractive, manufacturing, and logistics industries, the digital enterprise also involves OT.[8]

Companies have heavily invested in OT, much of it for increasingly smart machines and systems to automate discrete production tasks and continuous processes. This includes automation control and higher-level OT management platforms to efficiently operate, monitor, and optimize OT performance and maximize the utilization of capital assets.

Regarding IT-OT integration, many manufacturing companies have, in the past, implemented MOM. These systems provide up-to-the-minute (often near-real-time), accurate production-related information, such as overall equipment effectiveness, production costs, maintenance incidents, and quality status. For a while, the results were satisfactory, providing improved visibility and enabling better management of day-to-day operations, including scheduling adjustments where needed.

New challenges emerged, however, when globalization and outsourcing activities led to globally distributed production and supply chains. Since then, plant-focused MOM systems have not been sufficient because operations and KPIs must also be consistent across manufacturing lines and plants.

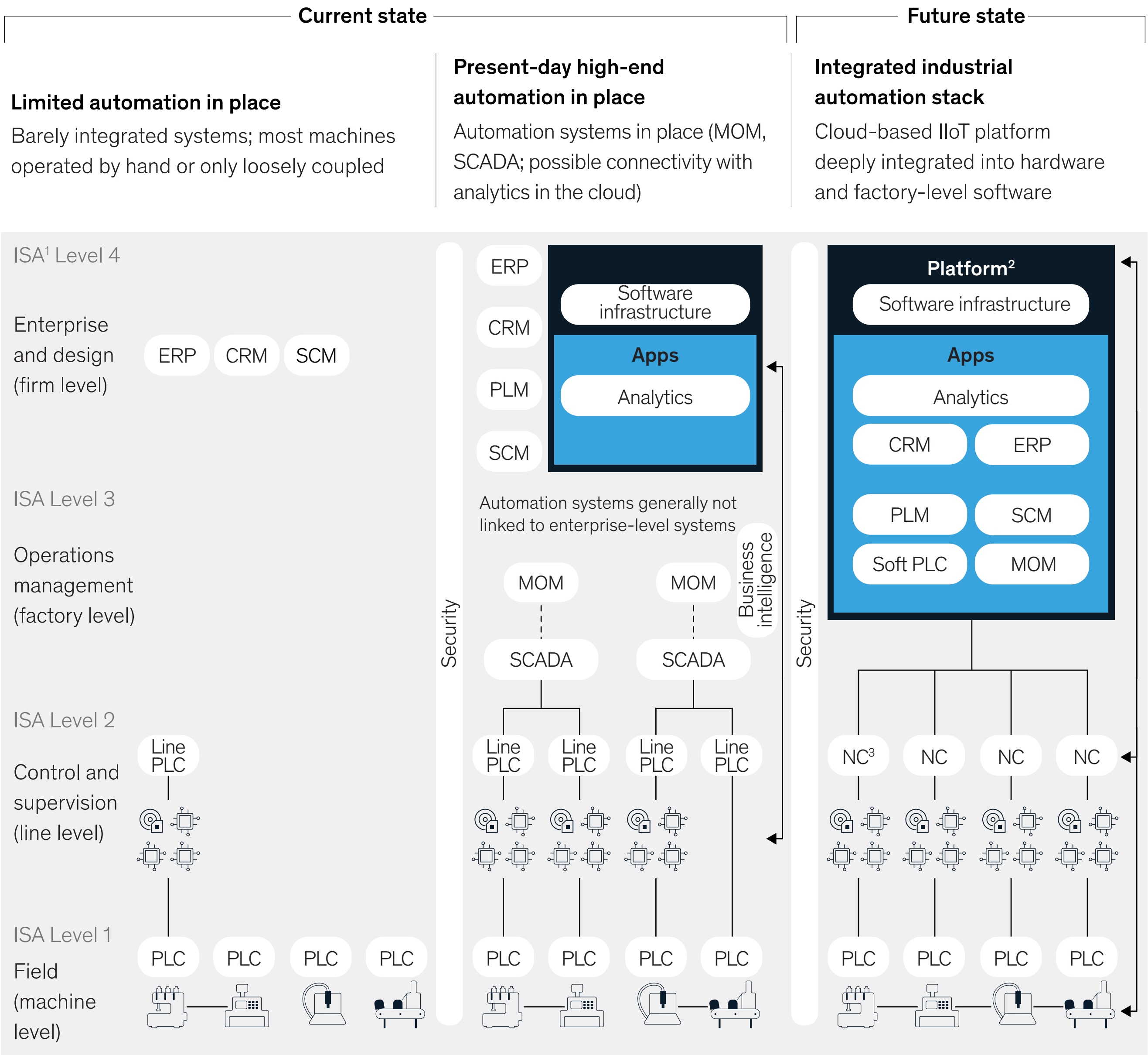
Capturing IIoT's full value potential requires more sophisticated integration approaches than current automation protocols provide

Connecting the two worlds of IT and OT would offer a truly end-to-end digital enterprise. Full integration of the two structures would lay the foundation for a fast, reliable, secure, and modern IIoT platform (Exhibit 21). But unfortunately for far too many organizations, sharing data between these two worlds can be a struggle, because their network infrastructures are neither up to date nor sufficiently connected.

[8] For further information on OT in general and the International Society of Automation's terminology and IT-OT integration standards (such as ISA-95) in particular, see: "ISA95, Enterprise-Control System Integration," International Society of Automation, 2020, isa.org.

Exhibit 21

The traditional stack will become interconnected and digitally enabled with an IIoT platform.



1. International Society of Automation
2. Can be hosted on site, as a company-internal service, or through a 3rd party
3. Numerical control

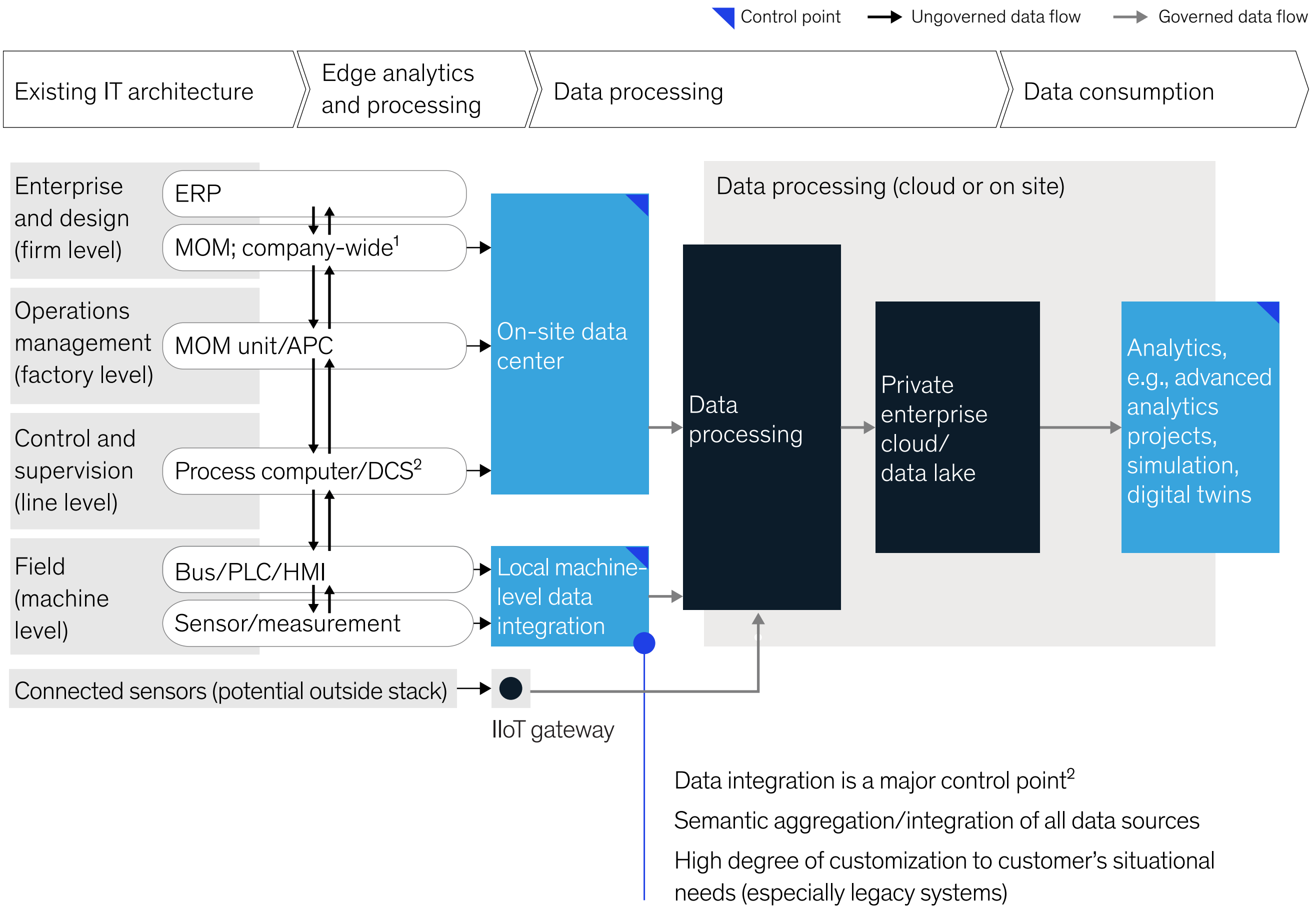
Source: McKinsey analysis

At the same time, manufacturers require not only information flows but also a data model standard with full transparency in all facilities and regions. They also require the control to put in motion and orchestrate operations across a heterogeneous IT, OT, and application system landscape and a distributed enterprise impacting the supply chain. Thus, there are still challenges with the traditional automation stack, particularly for discrete manufacturers. There are also issues that relate to the supporting data architecture. Specifically, at the company, factory, line, and machine levels, the data architecture must support all data activities from collection to processing to consumption (Exhibit 22).

Some of these challenges require software solutions, which a company may prioritize when making its architecture and digital manufacturing platform selection. Ultimately, a manufacturing company will need to decide how effective and responsive its operations infrastructure is and how well its performance supports the company's business strategy. Following an assessment of its current infrastructure, it needs to follow one of many paths toward a fully integrated automation stack.

Exhibit 22

The industrial automation stack requires suitable data architecture.



1. If existing.
2. Distributed control system.
3. Based on the current need for redundancy and latency, which is not a given at the moment for purely cloud-based solutions.

Source: McKinsey analysis

In view of this, the following four questions are central to the core platform design and cybersecurity. Each question is addressed in the corresponding four-step approach described below: [9]

— What are the gaps in operational data (OT system) integration in the current brownfield environment that need to be closed in order to implement the prioritized use cases?

— How can existing and newly added (IT system) applications and data sources be integrated into a common platform to make use of the data?

— Which vendor should be selected to implement the IIoT platform (or components thereof) and integrate data streams?

— How can cybersecurity challenges in IT-OT convergence be effectively managed?

Step 1: Fully assess the current brownfield setup in both OT and IT

Determining exactly where and how the current system falls short of enabling the prioritized use cases is an important initial step. Two main data sources exist that need to be assessed from a use-case and decision-making perspective—OT, which is found on the shop floor, ranging from sensors to PLCs and edge devices, and IT, represented by higher-level systems such as enterprise resource planning, supply-chain management, plant maintenance, MOM, and product life-cycle management.

A thorough assessment of the IT or OT tech environment is required along the technical dimensions of the IIoT tech stack (Exhibit 23), with the main focus on assessing technical integration options in terms of:

— Collection of operational data from functional systems, meaning those technologies that are available to capture, process, and transmit data from data sources in the plant

— Connectivity across different plant networks and machines in order to ensure secure links to the IT network and beyond

— Data infrastructure, meaning those technologies that are available to ingest, store, and transform data in various forms

— An analytics environment to deploy models across the data value stream, developed according to a standard for agile delivery

— An application environment to deploy transactional capabilities on data and insights, developed according to a standard for agile delivery

OT assessment is primarily concerned with two questions: which data sources are available on the shop-floor level and (how) should they be connected? Important dimensions to assess are:

— Available sensor data from machines and its characteristics (such as frequency, analog/digital, resolution, and required bandwidth)

— Available connections from equipment to the site environment (no connection, wired, wireless) and access characteristics (communications port, internal hard drive, communication protocols)

— Already collected data and contextualization (basis for decision making)

[9] In this context, see also: Eric Lamarre and Brett May, “Making sense of Internet of Things platforms,” McKinsey & Company, May 12, 2017, McKinsey.com.

Exhibit 23

The standardized IT-OT maturity assessment is the basis for a holistic, optimized architecture definition.

Main objective | Pre-steps for minimum viable product acceleration

Objectives

Define a target architecture and the concrete steps to implement the first minimum viable product initiative (go live) and summarize the improvements

Determine which areas lack digital integration and consider these areas in the target architecture definition

Diagnose the current state of the IT-OT maturity based on 5 factors: applications, analytics, data, collection, and foundations, to create a holistic view and define what needs to be part of the target architecture

Approach

Expert assessment of each site across 100+ nodes, analyzing end-to-end IIoT technology components and functional applications across key dimensions:

Applications
Technology to allow for custom visual and transactional applications for data and analytics

Analytics
Technology to catalog, share, and execute models encapsulating organizational expertise

Data
Technology to ingest, store, and transform data in various forms

Collection
Technology to capture, process, and transmit data from data sources in the plant

Foundations
Common technology capabilities and practices for cross-tier capabilities, incl. security, connectivity, networking, infrastructure, and governance models

Outcomes

Benchmarked findings across the full stack to consider in the architecture

Data and decision-making maturity assessment to identify gaps in capabilities for the future

Adjustments to the target architecture that consider the existing IT-OT software and hardware

Tactical guidance for prioritized minimum viable product use cases (steps for implementing the use cases while building the target architecture in parallel)

Source: McKinsey analysis

Typical challenges accompanying this assessment include the fact that there are multiple types of sensors, communication protocols, interfaces, and the like that need to be hosted on a common platform. This level of technical complexity requires the expertise of skilled OT architects, data architects, and data engineers. On the other hand, use cases might require data that is currently insufficiently measured or not measured at all (for example, vibration analysis in higher frequency bands) and therefore present the need to install additional sensor equipment.

A full gap analysis should be completed across the technology stack to ensure fundamental enablers are in place to achieve the value at stake and top-down business goals of the IIoT solution. Compound risk and the value at stake increase down the technology stack and into the OT systems that physically drive value.

The IT assessment is primarily concerned with the question of how to integrate legacy systems into the IIoT platform so as to enrich data and use existing interfaces. Automated equipment, MOM, product life-cycle management, enterprise resource planning, and more need to be integrated to achieve:

— **Product customization.** Rapid design and customization of a variety of products

— **Flexible production.** Efficient and mixed-line production for a variety of products

— **Value-added services.** Value created through big-data analysis

Achieving this might require a customized adapter to establish communication between legacy systems and the IIoT platform, with an emphasis placed on having correctly labeled data (especially time stamps) to make use of data in the data model on the IIoT platform.

Standards for interfaces, communication protocols, and so on exist and are codified in reference architectures, which are offered by IIoT platform providers. These offerings typically come with the benefit of having the entire IIoT platform supplied by one vendor with a common tech stack but cause vendor "lock in" and might fall short in areas that are not within the core competencies of the vendor. Based on the special circumstances of the current landscape, as well as strategic reasons, a "best-of-breed" approach might be followed, which is based on choosing the best solution per case or connection. This, however, leads to higher overall complexity (in maintaining the platform) and a higher total cost of ownership.

Step 2: Create the future target architecture to enable the use case

This step takes care of the design of the future target architecture in the technology stack. In terms of enabling data streams, this means defining the way to collect, connect, and ingest data from the shop floor to the IIoT platform.

Collection
The primary challenge when integrating historically siloed and functionally disparate data sources into an IIoT solution stack is the very different functional requirements between OT and IT systems. These differences can be largely traced to the characteristics of the data being produced and consumed: its required speed, relative importance, quantity, and complexity. Historically, OT systems have been closed off from IT systems, since they require high-speed deterministic and repeatable data transfers between purpose-built systems. Simply "plugging in" OT systems into larger IIoT solution architecture may lead to machine failure and security breaches in worst-case scenarios if the functional requirements of the three characteristics above are not thoughtfully considered.

With the integration of existing brownfield data sources being one of the major challenges of shop-floor digitization (see sidebar, "Overcoming the brownfield"), considerable effort has been made by platform, software, and specialized-equipment providers to allow access to available data. Standardized interfaces for most proprietary communication ports exist and are ready to be used for IIoT platforms, turning the former challenge from a prohibitively complicated issue into one that is still complex but solvable.

Furthermore, communication from edge devices to the platform and between devices on the shop floor will be harmonized with standards like OPC Unified Architecture. This vendor-independent, open standard for communication has been designated the de facto standard by all relevant industry segments and allows easy integration of edge devices based on clear publishing and subscription routines, while enabling the highest security and data standards. It includes modern, lightweight communication protocols like MQTT, effectively enabling connections to remote devices with a small code footprint at very low network bandwidths.

Overcoming the brownfield

The challenge in quickly connecting the brownfield shop-floor landscape to the IIoT platform is fundamental to implementing the IIoT platform. Although it is often sold as a matter of simple "plug and play," it should be approached with a carefully thought-out and clearly structured action plan. Getting it wrong will not only mean costly iterations and holdups, but quickly lead to frustration within the team and unwelcomed surprises in the later stages of the platform's implementation, such as erroneous sensor reads.

Based on lessons learned from the field, the following best practices can provide guidance for overcoming the brownfield successfully:

1) Clearly understand the data needs of the use case. Each use case will present a different set of data needs, which will in turn create requirements for available sensor measurements. Although the paradigm of "analyze everything" might be helpful in settings where data is already widely available, it is not feasible in situations where each data point might come with a price tag for a new sensor attached to it. Instead, teams should use their ingenuity to understand what data will be needed to realize the use case while keeping the nature of the machines and their physics in mind (for example, monitoring the condition of bearings using a vibration sensor). A master template should be created that contains all the required data types (units of measurement, data formats), measurement frequency, and storage means (for example, duration), as well as how they will be used.

2) Analyze the data supply of the machines to be connected. Each machine on the shop floor will carry a multitude of sensors, which are necessary for standard operation. Often, however, the sensor readings are not available to the outside, remaining within the internal control loops of the machine and its PLC. Though interfaces for data exchange exist, these might be locked by the machine vendor and remain inaccessible to the user, might not offer the needed bandwidth, might not allow for any continuous data exchange, or might simply be too old to connect to modern interfaces.

Only through assessing the available data based on the master template created in Step 1 can gaps be identified thoroughly. Additional sensors will then be needed, which offer the chance to create a more modern infrastructure, but might present the need to physically alter the machine and should therefore always be implemented with caution (warranties must also be considered).

3) Fill the gaps with robust solutions. Often, multiple solutions are available to fill identified gaps in the master template, like adding an additional hardware unit to a machine's PLCs, unlocking a machine's data interface through the machine vendor, or installing new sensors. For organizations to decide which solution to choose, they must consider purchasing costs, ease of implementation, and ease of use—but also the robustness of the solution itself. A new sensor might be cheap and will provide exactly the measurement needed, but might fail often due to unforeseen externalities (dust, for example). The chosen solution should be proven with a successful track record in the field.

Connectivity

Connectivity serves as a crucial enabler for any endeavor in the digital space, as it enables data to be transported from its source to where it is needed to generate insights. However, due to old infrastructure, connectivity often proves to be a main showstopper and needs to be tackled with the same diligence as the selection of data integration devices.

At present, manufacturing organizations are still mostly wired, but wireless connections are on the rise. In most of these instances, Wi-Fi is the wireless technology of choice, and with the advancement of Wi-Fi 6, it is getting closer to 5G in terms of functionality and performance. However, there are advantages to 5G: reliability of licensed spectrum, rich bandwidth availability with the introduction of mmWave, interference management, and standardized equipment, which ensures the expected level of performance regardless of the vendor or specification choice.

Wi-Fi can be expected to continue to play an important role, as it is a much more established ecosystem compared to cellular technologies today, and running a Wi-Fi network is much easier compared to a cellular network, as industrial verticals have no experience in cellular just yet. However, in cases where Wi-Fi is already reaching its limits today, many manufacturers are becoming interested in 5G—for example, in scenarios where there is a very large number of devices in a rather confined space, complex traffic, mission-critical functionality requirements, or a wide area to be covered. Wi-Fi is run on an unlicensed spectrum, and while this gives equipment and software providers much more flexibility on specifications, leading to more volatility in performance, licensed-spectrum 5G might be a better solution in the scenarios mentioned above.

Manufacturing players are intrigued by 5G because it simultaneously provides high speed, ultra-low latency, high reliability, and can support a large number of devices with various traffic types—all while saving on wiring costs and enabling true mobility for all devices (Exhibit 24).

That said, 5G will coexist with Wi-Fi and wired connectivity in the foreseeable future in industrial settings, enabling the next wave of IIoT applications and fostering automation. At the same time, this will inevitably increase the complexity of operations in the short term because, for example, manufacturing plants are not used to running cellular networks. This may change once deploying and running a 5G private network becomes as easy as Wi-Fi, but until then, an IIoT manufacturing landscape built on both 5G and Wi-Fi can be expected.[10]

Ingestion

Much of an IIoT platform's prowess is based on utilizing modern cloud solutions that offer tremendous potential for easily scaling processing power, enable modern data management solutions, and provide access to a wide variety of software solutions for data visualization, machine learning, and data analytics. Still, physical interfaces are needed to collect data from the shop floor. The hardware used to ingest data and send it to the IIoT platform needs to be connected to

---

[10] For a detailed discussion of 5G's future importance in the manufacturing space, see: Ondrej Burkacky, Alexander Hoffmann, Stephanie Lingemann, and Markus Simon, "The 5G era: New horizons for advanced electronics and industrial companies," McKinsey & Company, February 21, 2020, McKinsey.com.

Exhibit 24

5G delivers significant advantages over the connectivity technologies used by manufacturers today.

	Mobility	Adding devices/ sensors	Latency[2]	Jitter	Throughput	Spectrum[3]
Fixed network/ Ethernet	Limited by cable	Complex due to re-wiring	<1 ms	~40 µs	10+ Gbps	n/a
Wi-Fi 5	Provides lower range compared with 5G on the same spectrum	Easier than wired	~30 ms	<30 ms	~3 Gbps	Unlicensed Up to 120 MHz bandwidth
Wi-Fi 6			~10 ms	<10ms	10+ Gbps	
5G[1]	Provides	Easier than wired	<1 ms	10–100 µs	10+ Gbps	Licensed 100–500+ MHz bandwidth depending on the band

1. Assuming mid-band or mmWave
2. Test speeds are indicative; target real-life deployments of 5G are >20 ms depending on proximity of the devices and compute
3. Varies depending on region

Source: McKinsey analysis

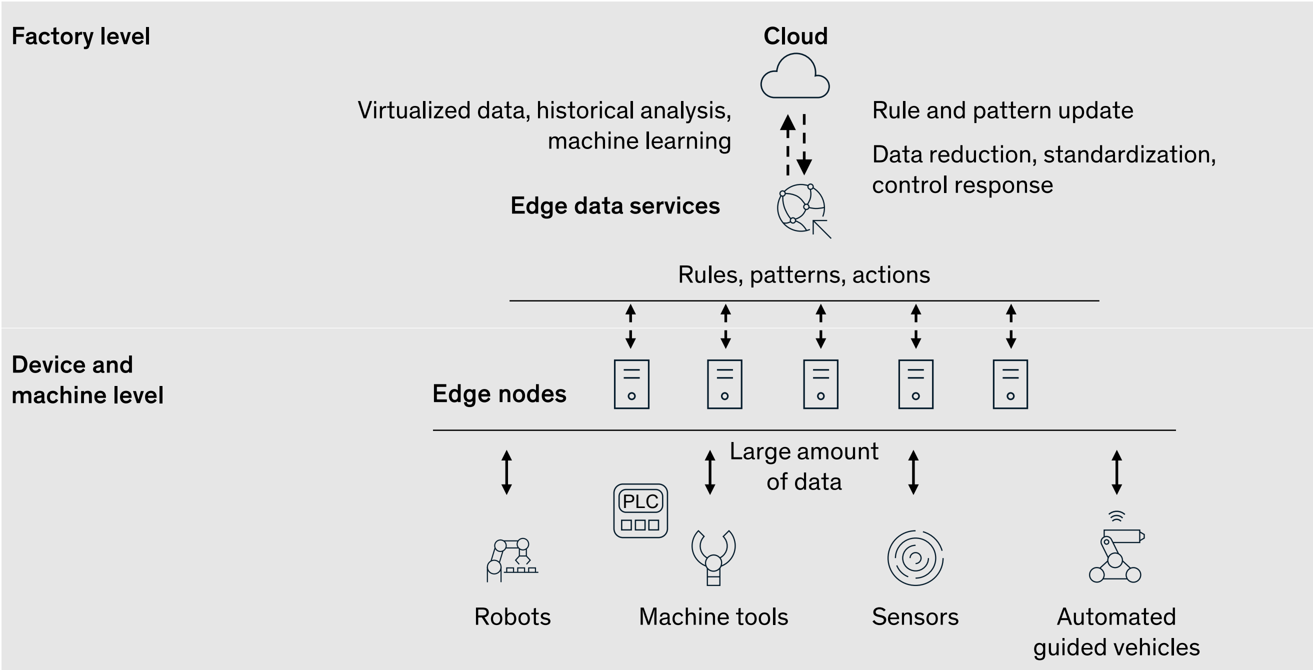
the devices (via cable or wirelessly) and must be able to communicate with both the device and platform. Due to limiting factors such as bandwidth, security concerns, or the need for instant computations in closed-loop systems, decentralization of processing power often becomes necessary, which upgrades ingestion devices from simple interfaces to capable processing units. These computation nodes are part of the so-called edge computing and typically deployed with a clear task allocation between what is processed on the edge and in the cloud (Exhibit 25).

Typically, a tiered approach is chosen, combining different types of edge computing and public clouds while integrating on-premises servers (see sidebars “Solving the real-time challenge with edge analytics” and “Considerations for edge computing in discrete and process industries”).

Exhibit 25

Future IIoT architecture utilizes the benefits of edge computing with clear task allocation on the edge versus in the cloud.

Company level



Edge intelligence	Technical benefits	Economic benefits
Real-time streaming analytics based on complex event processing (CEP)	Built for advanced, low-latency, closed-loop industrial applications	Faster actionable insights for greater operating efficiencies (uptime, yield, energy savings)
Iterative machine learning on live industrial data	Continuous inference on all sensor data (incl. video, audio) for closed-loop machine learning	Higher-quality predictive insights to drive asset performance and process improvements
Radically lower data persistence and transport requirements	Processing live data at the source reduces data networking and storage resources	Reduces cloud storage and communications costs by 100–1,000x
Enhanced security posture	Eliminates the need to transmit critical OT data across networks	Reduces security infrastructure, risk mitigation, and regulatory compliance costs
Cloud-agnostic	Avoids cloud provider lock-in and facilitates multi/hybrid cloud strategies	Increases bargaining power with cloud providers and reduces sourcing costs
Taps into OT tribal knowledge	Translates operator domain expertise into analytics expressions and machine-learning models	Cheaper and faster than PLC reprogramming, avoiding expensive cloud-based AI exercises
Utilizes small-footprint edge computing and controller hardware	Runs on industrial control systems or highly constrained edge computing devices	Minimizes investments in heavy computing or new industrial control systems hardware
Subscription-based pricing (not consumption-based)	Easier to project scaling requirements after initial proofs of concept	More controllable/predictable operating costs, radically cheaper for data-intensive apps

Source: Cisco; McKinsey analysis

Solving the real-time challenge with edge analytics

The technical decision on where and how to process data, and on how far it is transported, is closely connected to the question of each use case's latency requirements. On one hand, it might not be a problem to send a few kilobytes of temperature-measurement data to the cloud every minute or so in order to visualize it on a simplified dashboard. On the other hand, it might very well be physically impossible to stream a high-resolution video to a cloud platform, analyze it with machine vision, and send back results within a miniscule time frame in order to match certain process requirements. Physical transport is limited by the speed of light, bandwidth problems may arise, and processing might simply take too long to allow for "real-time" use cases with very low latency.

If data is to be used to meaningfully survey or control these tasks, then the entire process, from sensor to algorithm to control unit, needs to happen within a subsecond. Edge computing can be the solution that allows for very low latency while allowing for high flexibility, ease of use, and the processing power known from the cloud. Industrial PCs equipped with robust central processing and graphics processing hardware offer the needed computational power to analyze data streams very close to their origin.

Included in the IIoT platform, industrial PCs are equipped with capable software for analysis and communication within the platform environment. Modern IIoT platform providers offer ready-to-use software to include industrial PCs as edge nodes into the overall ecosystem, with user-friendly routines to set up and manage this decentralized processing power. Based on the latency requirements of each use case, core platform design must take the distribution of processing power on the edgeinto account. Different solutions are available that help solve the real-time challenge:

— **Data preprocessing on the edge.** The edge device serves as a communication node to the platform and helps transform "raw" high-bandwidth data streams into preprocessed lower bandwidth data that already carries more information (for example, by transforming raw vibration data into frequency spectrums). This overcomes bandwidth limitations and helps distribute computing power, while the actual insights are still produced in the on-premises or cloud servers.

— **Full analytics on the edge.** The edge device is fully capable of collecting and processing data from sensors, being equipped with not only the right hardware but also running complex software. When using machine-learning algorithms to get meaning out of the data (for example, machine vision with neural networks), a readily trained neural network runs on the edge device. Retraining—though possible otherwise—is often done on the cloud or on-premises servers.

— **AI-based control on the edge.** Given that modern edge devices are capable of analyzing data with very low latency, the next step of the evolution will be to use the decentralized intelligence to directly control processes within the production process. These closed-loop control systems based on edge analytics will enable the autonomous adjustment of process parameters to automatically correct deviations from the predefined process and mitigate defects before they occur.

In addition to edge devices—that are, after all, additional hardware components that might require maintenance—another potential solution for low-latency computation is offered by modern cloud providers in the form of local server distributions within mobile 5G networks. The cloud servers use the carrier's infrastructure and are deployed in a defined perimeter. Thus, physical data transfer via 5G uses the shortest ways possible to allow for very low latency. With cloud service providers also providing "on-campus 5G networks," customers are able to use these services within their own network to make full use of modern cloud infrastructure and 5G prowess.

Considerations for edge computing in discrete and process industries

Process industries typically have a distributed control architecture in place, with groups of supervisory controls, control rooms, and data-acquisition systems for production control—usually realized via multiple large screens and set-point input by operators to centrally steer distributed plant equipment and processes.

In the mid-1990s, the OPC Data Access framework was developed to allow standardized connection of Microsoft Windows–based equipment with the proprietary automation systems of multiple vendors. The framework has now evolved to the newer and more versatile version, OPC Unified Architecture, which allows connectivity with non-Microsoft Windows–based systems and subsystems.

Given OPC, edge computing has been standard practice for a long time, with value-added solutions and subsystems connected to distributed control systems. Very common are "plant historians": essentially, sophisticated Microsoft Windows–based data loggers. These loggers record all process data in a time series and store it for faster retrieval in the future.

Given these precedents, edge computing in process industries with local data processing is not a novel concept. Cloud computing, however, is. New solutions, using advanced analytics and AI, include cloning the plant-historian approach and connecting directly to a distributed control system via OPC Data Access or Unified Architecture. Data processing also occurs locally on the edge with minimum latency and delays and maximum efficiency.

In contrast to the process industry, discrete manufacturing shows a higher degree of OT decentralization. This is due to the higher number of specialized manufacturers and niche players that historically equipped their machines with specialized control units that allowed real-time data processing within the machine. As a result, the need for consolidation of data from a wide and heterogeneous data ecosystem is high, giving rise to new IIoT software offerings. One of these includes modern software middle layers with a wide variety of interfaces to different machines to enable data collection and ingestion.

Making edge solutions cloud compatible and seeking the best value from local and central data processing will be the path forward. One example of this is processing local data while simultaneously either benchmarking local performance against the performance of peer systems via the use of the cloud, or drawing other complementary information from the cloud for enhanced performance.

Step 3: Effectively manage cybersecurity challenges in IT-OT convergence

IIoT is dramatically boosting the number of connected devices deployed at industrial sites, the amount of data ingested routinely from such devices, and the degree of decentral and central aggregation and analysis of this data. As a consequence, these trends toward increased detail, connectivity, and aggregation can be expected to lead to significantly extended IIoT attack exposures.

In view of this, we have identified a number of characteristics of manufacturing companies that make OT difficult to protect:

— Legacy systems and inherent vulnerabilities in an organization's technology, including limited security mechanisms and logs, make OT particularly difficult to secure.

— Due to the high reliance on OEMs for the supply and management of OT, the ability of the owner to implement security for OT systems is limited (versus IT).

— Trends in vendor-management practices have increased the prevalence of remote connections and the number of third parties connected to the network.

— Within the organization, unclear ownership of cybersecurity for OT and undefined standards make applying OT cyber controls rather challenging.

— Low levels of cyber awareness among decision makers in the OT space and competing business priorities restrict the ability to implement OT security measures.

— The cybersecurity skills shortage is amplified for OT, where cross-skilled specialists are required.

— There are business and technical restrictions, such as the inability to shut down production lines to patch the old operating system or implement time-sensitive solutions.

Additionally, the concept of IIoT comprises four focus areas, each of which presents its own related security issue:

— Local area networks for collecting and locally processing data from connected industrial control systems
→ Security issue: lack of authentication and security in process sensors

— Transmission of data to the cloud via gateways
→ Security issue: lack of security in protocols and gateways

— Processing and storage of data in the cloud via appropriate platforms and specific algorithms such as big data
→ Security issue: lack of data security

— Interfacing between platforms and end users for monitoring
→ Security issue: lack of secure communication protocols

Compromised data can lead to equipment damage or other unforeseen operational problems, as well as regulatory issues and even personal safety hazards. This means that the cloud computing environment introduces security and operational challenges that need to be addressed, especially in OT environments that were never designed for remote access.

To bring in additional data required for big data analytics, IIoT applications and networks are generally built or augmented with existing industrial control system devices—and therefore inherit the lack of security of these devices. What's more, interconnected devices currently use custom protocols or gateways to get to universal protocols, such as OPC Unified Architecture. Unfortunately, however, these custom protocols or gateways are often developed without sufficient security considerations.

Deploying security controls across the entire organization also requires a sound understanding of the network architecture in both the IT and OT environments. This is because understanding the network architecture helps an organization better analyze where a threat is coming from and what controls need to be applied in the network architecture to repel the threat.

Against this background and in response to accelerating digitization with the convergence of IT and OT, more sophisticated cybersecurity functions are starting to transform organizations' capabilities along three dimensions: using quantitative risk analytics for decision making, building cybersecurity into the business value chain, and enabling the new technology operating platforms that combine many innovations.[11] These innovations include agile approaches, robotics, the cloud, and DevOps (the combination of software development and IT and OT operations to shorten development times and deliver new features, fixes, and updates aligned with the business).

Using quantitative risk analytics for decision making

Companies are starting to strengthen their business and technology environments with quantitative risk analytics so they can make better, fact-based decisions. This includes sophisticated employee and contractor segmentation as well as behavioral analysis to identify signs of possible insider threats, such as suspicious patterns of email activity. It also includes risk-based authentication that considers metadata—such as user location and recent access activity—to determine whether to grant access to critical systems. Ultimately, companies will start to use management dashboards that tie together business assets, threat intelligence, vulnerabilities, and potential mitigation to help senior executives make the best cybersecurity investments. As part of this dashboard setup, the following measures should be taken:

— A threat intelligence framework needs to be set up so that the organization can be up to date on the latest information on threats and be prepared to deal with them.

— Baseline security controls should be deployed across all layers of the organization's environments.

— Threat analytics and correlation solutions that can collect information across different environments should be leveraged to help the management team make decisions.

By taking these actions, companies will be able to focus on areas of the business that require the most protection, in the least disruptive and most cost-efficient way.

[11] In this context, see also: James Kaplan, Wolf Richter, and David Ware, "Cybersecurity: Linchpin of the digital enterprise," McKinsey & Company, July 19, 2019, McKinsey.com;James Kaplan, Chris Toomey, and Adam Tyra, "Critical resilience: Adapting infrastructure to repel cyberthreats," McKinsey & Company, January 15, 2019, McKinsey.com; Johannes Deichmann, Benjamin Klein, Gundbert Scherf, and Rupert Stuetzle, "The race for cybersecurity: Protecting the connected car in the era of new regulation," McKinsey & Company, October 10, 2019, McKinsey.com.

Building cybersecurity into the business value chain

Every digital company exchanges sensitive data and interconnects networks with customers, suppliers, and other business partners. As a result, cybersecurity-related questions of trust and the burden of mitigating protections have become central to value chains in many sectors, incorporating the following imperatives:

- The vision, strategy, and execution of a business plan need to include security, reliability, and safety. These should be part of the business planning process at all levels of all types of organizations (from IoT solution providers to customers).
- Security should be "owned" by one person at the executive level who is responsible for both IT and operations. Security policy, governance, and end-user education need to extend across the IT and OT environments as systems are interconnected.
- Technologies and threats across the IT and OT environments should be clearly understood, including the fact that technologies that work in the IT environment may not necessarily work in the OT environment and threats may be different between the IT and OT environments.
- The organization needs to understand that addressing risk across both the OT and IT environments includes the management of versions, status, last updates, control system versions, patch versions, and so on.

Importantly, regular risk assessments across all environments must be performed to identify vulnerabilities and ensure that the appropriate security controls are in place. Extending this imperative, leading companies are starting to build cybersecurity into their customer relationships, production processes, and supplier interactions. Some of their tactics include the following:

- Analyzing security surveys to understand what enterprise customers expect, and creating knowledge bases so that sales teams can respond to customer security inquiries during negotiations with minimum friction—for instance, one software-as-a-service provider found that its customers insisted on having particularly strong data loss prevention provisions
- Treating cybersecurity as a core feature of product design
- Educating employees on how to use digital channels and technologies safely and securely
- Taking a seamless view across traditional IT and OT security to eliminate vulnerabilities. One automotive parts supplier found that the system holding the master version of some of its firmware could serve as an attack vector to the fuel-injection systems it manufactured—with that knowledge, it was able to put additional protections in place
- Using threat intelligence to interrogate supplier technology networks externally and assess the risk of vulnerability
- Establishing robust controls for remote access and network segmentation and additional segregation within zones via virtual private networks

Enabling an agile, cloud-based operating platform enhanced by DevSecOps

Many companies seem to be trying to change everything about IT and OT operations at once to accelerate digitization: they are replacing traditional software-development processes with agile methodologies and, at the same time, repatriating engineering talent from vendors and giving developers self-service access to infrastructure. Some are even getting rid of their data centers altogether as they leverage cloud services.

Clearly, all of this is being done to make technology fast and scalable enough to support an enterprise's digital aspirations. Yet putting a modern technology model in place requires a far more flexible, responsive, and agile cybersecurity operating model. Key tenets of this model include:

— Shifting the talent model to incorporate those with "e-shaped" skills—cybersecurity professionals with several areas of in-depth knowledge in IT-OT convergence, such as in integrative problem solving, automation, and development—as well as security technologies.

— Moving from ticket-based interfaces to APIs for security services. This requires automating every possible interaction and integrating cybersecurity into the software-development tool chain. That will allow development teams to perform vulnerability scans, adjust data loss prevention rules, set up application security, and gain access to management services.

— Organizing security teams into agile, scrum, or scrumban teams that manage developer-recognizable services, such as identity and access management or data loss prevention. Also, recruiting development-team leaders to serve as product owners for security services can help, just as business managers are product owners for customer journeys and customer-oriented services.

— Tightly integrating security into enterprise end-user services so that employees and contractors can easily access productivity and collaboration tools via an intuitive portal.

— Building a cloud-native security model that ensures developers can access cloud services instantly and seamlessly within certain guardrails.

— Collaborating with infrastructure and architecture teams in IT and OT to build the required security services into standardized solutions for massive analytics and robotic process automation. These solutions comprise the following:

  - Next-generation IT and OT host-based intrusion prevention and detection systems, including all IoT and IIoT protocols
  - Anti-malware and ransomware protection for both IT and OT environments
  - Whitelisting for both IT and OT environments
  - Network sandboxing technology that can analyze and monitor for vulnerabilities and threats on the different types of IoT protocols without affecting operational processes
  - Encryption technologies for providing authentication and verification, which are a must across all IoT devices and control systems
  - Technology for managing versions of devices, control systems, patches, and the like across both IT and OT
  - APIs that can be directly integrated into devices
  - Security capabilities in the form of software development kits or application programming

All these actions have proven absolutely necessary for the security of an organization. Without them, cybersecurity breaches occur more frequently—and often, with more severe consequences. The needed actions, however, exist in tension with the emerging digital-enterprise model—the outcome of an end-to-end digital transformation—from the customer interface through the back-office processes. As companies seek to use public cloud services, they often find that security is the "long pole in the tent"—the most intractable part of the problem of hosting applications on public cloud infrastructure.[12]

Step 4: Select a partner rather than a vendor to help implement the platform

Given the complexity of creating a target architecture and choosing the right technical configuration of the IIoT platform, it is not surprising that vendor selection for the platform is a major step toward successful implementation. As with all major decisions, vendor selection must be based on a structured assessment of different alternatives. In the search for the perfect implementation partner, the following platform dimensions should be carefully assessed:

— **Business model.** Does it enable customers to create their own offering? How does it enable scaling? Who owns the data?

— **Market readiness.** Is the pricing model understandable? How effective is the organizational setup?

— **Use-case offering.** Do successful, fully implemented lighthouse cases exist?

— **Existing development capabilities.** How invested is the provider in developing the platform further? Does a vivid developer community exist?

— **Technology.** How open and modular is the platform? Does it offer an advanced security plan?

— **Operations.** How advanced are release management and update control? How frictionless is support?

The right partner should be selected based on criteria that not only contain pricing and technical dimensions, but also sustain a competitive edge for future developments. This can be evaluated by looking closely at partnership components, such as the partnering strategy (What is the strategy for finding partners who provide their own services and solutions through their platform?), development capabilities (How invested is the provider in developing the platform further?), and integration into the developer community (Is there an active developer community that provides its own apps, assets, or solutions on the platform?).

3.2 IIoT platform: The cloud imperative in manufacturing

The common industry approach to the cloud refers to the replacement of key IT activities, access to on-demand infrastructure, provisioned computing, storage, database services, and more. While all these descriptors are accurate, organization leaders often hear them and lose sight of the broader impact that the cloud can have on transforming the full IT operating model and, most importantly, on the business.[13] Consequently, when they set out to write a business case, they spend months analyzing on-premises costs compared with cloud costs and focus much less time on the main value driver of the cloud: the business benefits.

[12] "Cybersecurity: Linchpin of the digital enterprise," July 19, 2019.
[13] In this context, see also: Joe Dertouzos, Ewan Duncan, Matthias Kässer, Satya Rao, and Wolf Richter, "Making the cloud pay: How industrial companies can accelerate impact from the cloud," McKinsey & Company, October 1, 2020, McKinsey.com.

Many industrial companies face challenges from overly complex systems. For instance, one company undertook a journey to rationalize more than 30 enterprise resource planning systems it had accumulated over a series of acquisitions. This complexity limited transparency and slowed processes for manufacturing, supply chain, and other business functions. Data that could help the company improve the business existed only in spreadsheets and systems scattered throughout the organization. Scaling up any idea to create a real impact required a multiyear program.

Using the cloud to solve such business challenges has not been easy. Many cloud migrations have failed because they did not first simplify the IT landscape and establish data governance. Furthermore, extra costs have often threatened financial success:

- Switchover costs for simultaneous cloud and on-premises data center operations result from complex applications and an unwillingness to migrate quickly.
- Hidden costs may arise when platforms, tooling, and services are not well understood and supply and demand is not actively managed.
- System-integrator costs may continue into the third or fourth years after the switch to the cloud, incentivized by a time-and-materials model.
- Costs of add-on services can be three to four times higher than necessary if applications are not well configured.
- Financial-accounting rules and poor governance can exacerbate these costs, or create additional costs by writing down nondepreciated IT assets.

However, while the majority of cloud costs are in IT, most of the value is generated on the business side (Exhibit 26). The cloud provides access to innovations from cloud providers, such as new AI and machine-learning engines. Second, the cloud facilitates experimentation with new products and features, since the cost to set up a “sandbox” environment is nearly zero. It also links the business with new products and services, such as sales tools, from the partner ecosystem, which dramatically lower barriers to collaboration.

On-premises and even hosted (private cloud) platforms cannot keep up with the ever-increasing complexity and demands of modern manufacturing. The manufacturing and supply chain employees, including external participants (customers and suppliers), need timely and controlled access to operational and business data for better-informed decision making. IIoT cloud platforms provide this ubiquitous access and connectivity.

The intrinsic benefit of cloud systems is operation with a single source of truth, eliminating disparate tools and data silos, and consequently avoiding manual input or delayed syncing of data. This results in a reduction of the amount of errors, bottlenecks, and basic tasks when streamlining processes and workflows.

The cloud offers potential for IT efficiencies, although they may not overcome the cost of the cloud alone. Labor efficiencies are created as cloud-standard instrumentation increases development productivity by enhancing software-engineering practices and driving automation in application development and maintenance, development-security operations, infrastructure, and tickets and support. Nonlabor efficiencies arise from the smaller number of on-premises data centers, lower spending on hardware (also due to standardization), and the rationalization of new applications when legacy applications are retired. Furthermore, cloud offerings can also enhance OT, by making data from OT devices available across physical locations and addressable by powerful cloud computing for machine learning and AI.

Exhibit 26

The majority of cloud costs come from IT, but the value mostly comes from the business.

Key elements of the cloud business case

IT cost

Major cost categories	
Running costs	● **(Hybrid and multi-)cloud consumption costs** (incl. "cloud roaming"—costs to synchronize multiple cloud environments)[1] ● **Legacy systems continuing operation** Increased network costs in hybrid cloud models Retaining cloud talent—but often also old infrastructure teams
Migration costs	● **Internal migration costs, incl. "double bubble" costs for parallel infrastructure during migration** External migration costs, e.g., system integrator Up-front, one-time investments (e.g., in capability building on the business side, IT asset modernization) Data management costs

● Mission critical for a positive business case—requires proactive management

Business value

Sample use cases		
Sales, admin, and support	General and admin	Fraud and debt analytics Analytics-driven accounting and IT
	Marketing and sales	Lead generation Marketing budget allocation
	Aftersales	Predictive service/ intervention Customer service management
Product data	R&D	R&D data mining Project portfolio mgmt platform
	New services and business models	Hardware as a service On-top services/ connected products
OT	Manufacturing	Predictive maintenance Visual inspection/ quality control
	Supply-chain management	Intelligent route planning Vertical supply-chain integration (just-in-time)
	Procurement	Spend analytics Raw-material price modeling

Expected impact on EBIT margin[2]	IT cost	Business value
	~0.2% pts	**~9% pts**

Current cloud programs mainly focus on IT infrastructure substitutions, leaving business value mostly untouched

IT infrastructure substitutions are often not as effective as promised—complex and hidden cost structures of cloud migrations and operations often lead to uncompelling business cases if not properly managed; even success cases only break even in years 3–4

1. Frequently underestimated, databases can often be significantly more expensive (up to 10x) in the cloud; cloud databases lack cleansing functionalities, leading to higher storage costs compared to on-premises databases
2. Estimated potential for a typical automotive player by 2025 from the cloud as an enabler for advanced analytics, a new business model, improved operational efficiency, etc—investments are not included

Source: McKinsey analysis

Step 1: Make the cloud pay off in the short term

Industrial companies can “bend the curve” to make the cloud pay off in the short term. This requires four actions (Exhibit 27):

- Be strategic and sequenced about which applications to migrate to the public cloud and which applications need to remain in the private cloud or on premises (edge), and then manage cloud consumption. The end-state vision should determine which applications and data should migrate and which should stay. Cloud operations can be adopted in multiple environments, not just in the public cloud.
- Start changing the IT and OT operating model early to drive a significant change in pace and productivity, especially in DevSecOps and infrastructure management. Use the software-engineering paradigm to enhance the productivity of IT people spend.
- Balance infrastructure migration against an ongoing cloud-enabled business redesign, since the latter can start to self-fund the transformation. The redesign may include Industry 4.0 tools and the integration of OT, new analytics, or new business models. Emphasize business-process improvements, often enabled by analytics, where investment is lower and impact is faster.
- Embrace the flexibility of the cloud to drive ongoing business innovation in the form of faster introduction of new products, more partnerships with external players, and new ecosystem plays.

Step 2: Tightly manage and control the cloud transformation

Managing a cloud transformation requires strong governance. Critical activities include the following:

- Quantifying business benefits for each initiative of the transformation program
- Planning and executing an end-to-end transformation by business domain, rather than focusing on individual use cases
- Preparing the legacy application and data landscape ahead of the transformation; this includes the establishment of strong data governance
- Integrating application rationalization and retirement into the transformation governance
- Training the entire relevant organization by domain
- Establishing a consistent and sustainable governance model between IT and the business functions, including central (corporate) and decentral functions (for example, IT and OT at the manufacturing sites)
- Implementing an agile process from demand management to delivery
- Ensuring the adoption of operational improvements by investing in change management from the very beginning, getting commitment from the business functions, such as supply chain and manufacturing, and aligning IT and OT

Exhibit 27

A proven approach to scaling up cloud transformations comprises four steps.

Illustrative

Diagnose	Plan/reset	Set up foundation	Scale and transition
Conduct a quick diagnostic to evaluate the current cloud maturity level and identify capability gaps: – Assess the organization's progress toward goals – Identify full potential and bottlenecks	Develop the cloud strategy Build the business case – incl. domain-specific business benefits (e.g., access to innovation, agility, resiliency) and technology cost benefits (e.g., labor productivity, application rationalization) Determine and design future operating models for business and IT Build an implementation road map to assess the value of business benefits Design future-state architecture and tooling needs	Set up the transformation program, incl. IT and OT, business functions (e.g., manufacturing, supply chain), and enabling functions (e.g., finance, HR) Enable an enterprise-wide cloud operating model allowing IT and the business to take full advantage of the cloud Guide the building of the technology backbone for the cloud Identify and execute minimum viable products to demonstrate success Build capabilities and responsibilities with the internal team	Drive business change and innovation Accelerate cloud migration and enterprise-wide upskilling Mature the cloud operating model

Source: McKinsey analysis

The idea of infrastructure as a service—that an external provider will manage an organization's underlying network, hardware, and resources—is an exciting proposition for many organizational leaders. A misconception arises, however, when leaders interpret infrastructure as a service as a full replacement for their infrastructure organization. While the cloud radically changes the activities, talent, and operating model required in an internal infrastructure group and beyond, it does not altogether replace the need for infrastructure management.

Companies must ground the new partnership between IT and the overall business areas in an operating model that reflects and supports their growing investment in the cloud. Here, it will help to think about an integrated system rather than a set of individual technologies. Doing so implies organizational change across all of IT, and many of the business units and functions as well. This operating model combines cloud-based digital technologies and agile operational capabilities in an integrated, well-sequenced approach that can rapidly accelerate digital strategy and transformation.

Step 3: Set up an infrastructure team that can operate much like an app development team

When companies transition to the cloud, they will encounter hundreds of services that can be combined and configured to affect performance, security, resiliency, and more. They need an infrastructure team that can build and manage standard templates, architectures, and services for use by their development teams. As infrastructure in the cloud is managed through code, this infrastructure team will require different skill sets (for example, committing code) so they can operate much like an app development team. Without this infrastructure team creating standardized services and platforms, many enterprises will simply replicate the fragmentation and chaos they experienced with on-premises solutions.

To accommodate this shift in function, infrastructure organizations must transition to a proactive (rather than reactive) operating model. Instead of responding to customization requests from development teams, which take months and can quickly become costly, cloud infrastructure teams should proactively consider organizational needs. In doing so, the ownership lands more squarely on development teams themselves, who have more flexibility in quickly configuring the resources they need. Not only will the teams gain more direct responsibility over costs, but this increased flexibility will also lead to greater productivity and speed.

Shifts in infrastructure are not only helpful in managing the cloud but also necessary in order to see the full range of cloud benefits. In general, traditional infrastructure teams running a cloud would be too large and costly, and would miss the benefits of having app teams share responsibility for the running costs they incur. However, having no infrastructure team at all would wreak havoc on an organization's ability to manage and benefit from the cloud. Instead, a leaner, more specialized infrastructure organization is required to achieve the full range of agility, innovation, and performance benefits that the cloud can offer.

3.3 Tech ecosystem

Not every company will succeed by orchestrating ecosystems. For many, joining existing ecosystems will be more effective. Whichever approach they choose, however, companies will need to start developing new capabilities—from "ecosystem IT" systems that link enterprises to platforms and innovative third-party services, to new management skills that can handle the scale and complexity of ecosystem relationships. To win, companies will need to embrace new relationships and ways of collaborating.

Companies have always forged partnerships and alliances, but because ecosystems are on such a large scale, traditional approaches to relationship management are not applicable. Successful companies are finding new ways to choose and manage partners and make deals. Three steps are of particular importance in this context: [14]

[14] In this context, see also: Jürgen Meffert and Anand Swaminathan, "Management's next frontier: Making the most of the ecosystem economy," McKinsey & Company, October 27, 2017, McKinsey.com.

Step 1: Understand the key elements of a sustainable ecosystem

To be successful, an ecosystem must have a compelling value proposition that is attractive, open, and relevant to multiple businesses. Today's dominant ecosystems were launched by ascendant tech companies, which have used hyperscale platforms to compete with, disintermediate, and often substitute the offerings of traditional competitors by controlling customer interfaces and control points.

In order to get value from IIoT enabling an ecosystem, it helps to have a platform on which to create and manage applications, run analytics, and store and secure data. Ecosystem partners, businesses, and developers have a bewildering array of platform options to choose from, which may have very different capabilities.

The preferences of IIoT leaders suggest a greater willingness to draw capabilities from an ecosystem of technology partners, rather than rely on homegrown capabilities. When it comes to choosing the IIoT platform that will best meet their needs, IIoT leaders follow an approach that is different from that of laggards. Beyond the interest in software-development environments supported by IIoT platforms, leaders are more likely to choose IIoT platforms according to whether they attract and support a vital community of third-party developers. Perhaps because these capabilities are so sophisticated, leaders are more likely than laggards to turn to outside partners for their IIoT platforms.

Step 2: Choose the right partners with a view to achieving balanced partner diversity for the platform-enabled ecosystem

Any effective ecosystem strategy depends on understanding where the value is. Calculating the value of assets, such as customer relationships and proprietary data, and existing capabilities and where market opportunities are emerging, reveals the clearest picture of where this value lies. Equipped with that baseline, organizations can evaluate collaboration opportunities with an eye for capabilities, markets, and technologies that complement and support their strategic ambitions.

Any temptation to narrow the search for collaboration opportunities with organizations within the same sector or region should be resisted. A better approach is to systematically map ecosystem partners across industries and archetypes, identify key criteria (such as access to new customers or capabilities), and consider likely trade-offs (such as domain expertise, lock-in effects, and market potential).

In this context, companies should keep four key considerations in mind: Would adding this company help build an ecosystem with a diverse and complementary set of skills and value propositions? Is its business model sufficiently nimble, customer-focused, and future-proof? Are its staff and management team highly effective? Is it culturally compatible in terms of its way of working?

As the ecosystem market consolidates, companies should try to find a partner who is either large and will be in it for the long run or is highly focused, distinctive, and successful in solving their most difficult problems. Companies must look at the whole technology environment, not just the applications.

What they also need to be aware of is that the level of diversity of the targeted ecosystem can vary: it may range from being rather monolithic with only a handful of solution vendors and support services, to being highly fragmented, with hundreds of hardware, software, and support service providers (Exhibit 28). Regarding the composition of the software, hardware, and services required for supporting application verticals and platforms, three levels of diversity can be distinguished:

— Choosing best-in-class players for each category of hardware, software, and support required (see Archetype 1: Diversified in Exhibit 28) will help lead to optimal results within the respective category; however, the support burden, the effort required for integrating the various categories, and the number of potential points of failure will increase significantly.

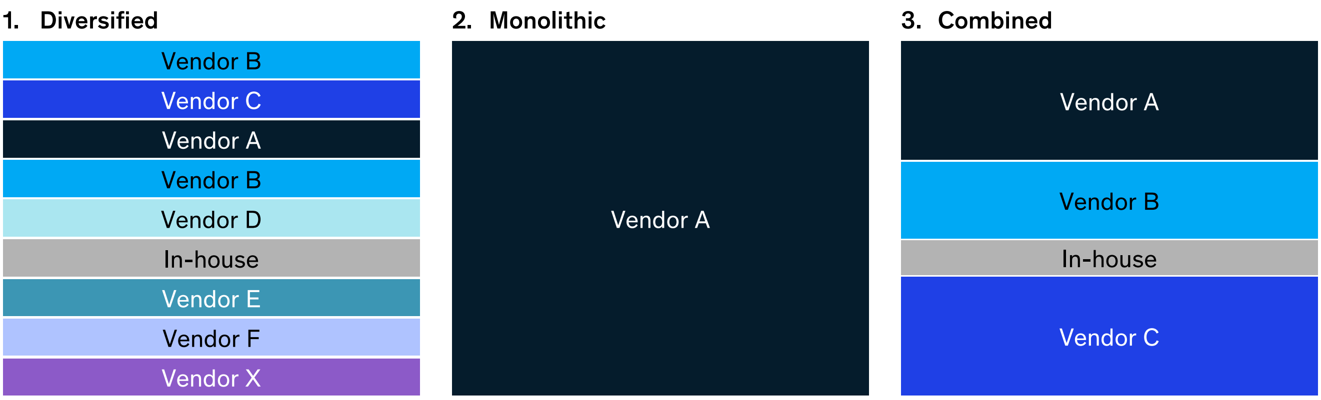
— Minimizing diversity in the technology stack (see Archetype 2: Monolithic in Exhibit 28) has the benefit of reducing the support burden, simplifying the integration between disparate systems, and reducing the quantity of potential failure modes. Conversely, adopting a more monolithic solution ecosystem can lead to vendor lock-in and a reduced ability to meet the changing needs of end users and the enterprise.

— Taking a hybrid approach (see Archetype 3: Combined in Exhibit 28) balances the needs of the business with the costs of implementation and operation while still leveraging best-of-breed technology solutions that can be integrated into a more holistic ecosystem. The needs of the business and the end consumers of the IIoT solution and its underlying architecture must be carefully weighed against short- and long-term goals, the effort of implementation, and the value at stake.

Exhibit 28

The three ecosystem landscape-archetypes differ in their levels of diversity.

Aspects of the IIoT platform solution



Not favorable due to the effort of vendor coordination and different interfaces

Infeasible, since no single vendor covers the whole IIoT stack and there is a high risk of lock-in

Strikes a balance between efficient sourcing and avoiding lock-ins

Source: McKinsey analysis

The level of diversity for most best-in-class players generally falls within the middle of this range, with greater consolidation across the platform and enabling building-block categories. This provides a unified pipeline for the development and support of purpose-built applications—be it for optimization of the production planning process in terms of raw-material costs and scheduling or for maximizing throughput of manufacturing lines while minimizing waste.

What's more, platforms (such as for enterprise planning, machine connectivity, and industrial wearables) and their enabling building blocks (interfaces, connectivity, and security) are often shared across application verticals, while end applications are often use-case and end-user specific.

Tactical solutions often lean toward a more monolithic ecosystem; however, most IIoT solutions tend to be diverse by nature, primarily driven by the complexity of industrial automation systems and their supporting OT.

Step 3: Implement business development teams as a structure to manage the complex ecosystem and ensure agility

In order to leverage the contributions of those platform and solution players, leading companies are putting in place ecosystem business development teams that are similar to central sales teams in business-to-business companies but also include executives and managers from corporate development, management, legal, business development, and technology. Involving legal specialists in negotiating teams is particularly important, given the host of questions raised by working with third parties—questions about cybersecurity, intellectual property, data ownership, licensing, privacy, profit sharing, liability, regulatory compliance, and customer management.

Companies are also likely to need people with uncommon technical skills, such as full-stack IT architects who can integrate multiple technologies across infrastructure, apps, and services. The main responsibilities of an ecosystem business development team are to continuously review companies, reach out to prospective partners, and screen likely candidates for compatibility. The team should put a pipeline in place to track progress and hold frequent reviews at specific milestones to determine whether and how to pursue promising options and when to drop unsuccessful efforts. The team also decides how new relationships should be structured—as joint ventures, mergers, or partnerships—depending on competitive pressures and market opportunities.

Managing ecosystems requires a balance between standardization (to prevent a chaotic mess) and flexibility (to capture opportunities fast). Standardizing core processes such as pipeline management, negotiation templates, and software acceptance guidelines can help accelerate the development of a successful ecosystem. At the same time, putting tools in place to track performance in real time, establishing flexible agreement structures, and investing in agile processes can give companies the flexibility they need to adapt to the changing dynamics of ecosystems.

Investing in open-IT architecture, APIs, and microservices will be key to developing a technical platform capable of supporting the level of flexibility and agility needed in ecosystems. In addition, organization leaders must role-model desired behavior, such as treating ecosystem management as a top priority and spending time with external partners.

Outlook: How to get started on a digital transformation in manufacturing

The “framework for success” in Chapter 2 describes the seven-step enabler process of ensuring sustainable transformation success. For organizations to bridge the gap between where they are now and Step 1 of the transformation process, certain elements need to be taken into consideration before embarking on the transformation journey. For this, there are seven pragmatic recommendations:

1. Secure sponsorship from the CEO to drive digitization and make it a high-priority, firmwide project.
2. Set a bold aspiration up front for a new way of working, and clearly communicate the value expected from it.
3. Identify and rapidly prove the value for a “core set” of eight to ten high-impact use cases.
4. Define lighthouse use cases strategically to capture a significant share of the potential IIoT value and self-fund the transformation.
5. Build a flexible IT architecture and an ecosystem of technology suppliers to rapidly scale up use cases.
6. Recognize the need for nontraditional talent and recruit or build capabilities accordingly.
7. Acknowledge that less than one-third of the overall success can be attributed to technology, while the remaining two-thirds hinge on process, organization, and capability transformation.

A holistic approach to digital manufacturing—one that considers the fundamentals of the organization and the business as much as it focuses on the technology-related factors—can help manufacturers overcome the hurdles that stand between pilot success and company-wide rollout. If approached correctly, substantial value can be created by a digital transformation, as has been demonstrated by several real-world cases.

Glossary

The definitions in this glossary reflect how the respective terms are used and abbreviated in this report.

5G. 5G is the fifth-generation technology standard for cellular networks, which mobile network operators began deploying in 2019. Development of a new standard coincides with the addition of new spectrum bands opened for cellular usage (high-frequency radio waves, 28 GHz+), which 5G can utilize in addition to the spectrum bands previously assigned for cellular usage. This newly introduced spectrum offers a lot of new bandwidth, enabling the high speeds and low latencies required for advanced use cases; however, it requires a very dense deployment due to the short range of the wave and worse propagation compared to mid-bands (>6 GHz). Beyond mobile operator networks, 5G is also expected to be deployed for private networks with applications in IIoT, enterprise networking, and critical communications.

Advanced analytics. Advanced analytics is the autonomous or semiautonomous examination of data or content using sophisticated techniques and tools, typically beyond those of traditional business intelligence, to discover deeper insights, make predictions, or generate recommendations. Advanced analytic techniques include data and text mining, machine learning, pattern matching, forecasting, visualization, semantic analysis, sentiment analysis, network and cluster analysis, multivariate statistics, graph analysis, simulation, complex event processing, and neural networking.

Advanced automation. Advanced automation refers to sophisticated automated systems, ideally with the additional capability for self-maintenance and repair, requiring little to no human interaction to operate, apart from top-level guidance. Not being reliant on human effort to scale up, these systems hugely magnify production capabilities and decouple human time and effort from industrial productivity.

Artificial intelligence (AI). AI is the study of “intelligent agents”: any device that perceives its environment and takes actions that maximize its chance of successfully achieving its goals. Alternatively, AI can be characterized as a system’s ability to correctly interpret external data, learn from this data, and use that knowledge to achieve specific goals and tasks through flexible adaptation.

Brownfield. Brownfield development is a term commonly used in the IT industry to describe problem spaces requiring the development and deployment of new software systems in the immediate presence of existing (legacy) software applications or systems. This implies that any new software architecture must take into account and coexist with live software already in situ. The same applies to operational technology (OT) where the term brownfield usually refers to an already existing and operational manufacturing setup with running OT.

Closed-loop (control) mode. Fundamentally, there are two types of control loops: open-loop control, and closed-loop control. In contrast to open-loop control, where the action from the controller is independent of the process output (or controlled process variable), the action from the controller in closed-loop control is dependent on the process output. A closed-loop controller therefore has a feedback loop which ensures the controller exerts a control action based on the measured parameters from the process output.

Cloud computing: Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the internet. Large clouds often have functions distributed over multiple locations from central servers. Clouds may be limited to a single organization (enterprise or private cloud), or be available to many organizations (public cloud). Cloud computing relies on the sharing of resources to achieve coherence and economies of scale. Advocates of public and hybrid clouds note that cloud computing allows companies to avoid or minimize up-front IT infrastructure costs. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and that it enables IT teams to adjust resources more rapidly to meet fluctuating and unpredictable demand.

DevSecOps. This is an augmentation of the DevOps approach to allow for security practices to be integrated. The traditional centralized security team model must adopt a federated model, enabling each delivery team to factor the correct security controls into their DevOps practices. DevOps itself is a set of practices that combines software development with IT operations to shorten the time to market, enable continuous delivery, and improve software quality.

Distributed control system. Complex automated industrial systems used in discrete manufacturing and production processing require a distributed control system in order to operate. Organized as a hierarchy, a distributed control system starts by linking the various components—actuators, contactors, motors, sensors, switches, and valves—that do the work at the field level (such as on the shop or production floor) to PLCs. In turn, PLCs are connected to a human-machine interface, typically a display of some kind that enables human operators to monitor overall system performance and component behaviors and, if necessary, adjust parameters accordingly.

Edge computing. In contrast to cloud computing, edge computing refers to decentralized data processing at the edge of a network. It is the result of moving computer applications, data, and services away from central nodes (data centers) to the outer edges of a network. In other words, the aim is to process data streams as close as possible to their origins and thus grant lower latency than would be possible if data had to be sent to a cloud server first.

Enterprise resource planning. Enterprise resource planning is a software system that integrates information across an organization, incorporating supply chain data, inventory, sales and service orders, and customer information. This system facilitates the flow of information between all business functions and manages connections to outside customers.

Global Lighthouse Network. The Global Lighthouse Network is an ongoing research collaboration between McKinsey and the World Economic Forum, whose latest insights show that organizations that are leaders in applying Industry 4.0 technologies are benefiting from their head start and generating even more value across their entire enterprises, not just within factories. A detailed look at lighthouse success cases reveals organizations that are driving outsized improvements in productivity, sustainability, operating costs, and speed to market.

Graphics processing unit. A graphics processing unit is a specialized, electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device. Graphics processing units are used in embedded systems, mobile phones, personal computers, workstations, and game consoles. Their highly parallel structure makes them more efficient than general-purpose central processing units for algorithms that process large blocks of data in parallel, which makes them ideal candidates for machine-learning tasks.

Infrastructure/platform/software as a service. In cloud computing, a general distinction can be made between three cloud service levels, which build on each other: infrastructure as a service, platform as a service, and software as a service. Infrastructure as a service offerings usually include the server instance for computing, storing data, and networking functionality.

Platform as a service adds a development environment within the cloud platform in addition to the server instance to enable companies to program applications. Software as a service offerings include readily available software that is hosted and managed on a cloud. What all three levels have in common is that abstract or virtualized IT infrastructures are provided. This means that infrastructure, platform, and software as services, like all cloud computing services, can be dynamically adapted to the needs of users or companies at any time.

Industrial Internet of Things (IIoT). IIoT is the use of IoT technology in an industrial setting, usually in a business-to-business environment and often focusing on areas of operations, such as manufacturing, supply chains, and logistics.

IIoT-enabled backbone. At the heart of IIoT lie reliable, high-performing communication and connectivity networks. It takes robust and flexible communication networks to realize the vision of machines that talk to each other, collect data, and analyze and report on that data. In industrial operations, the physical assets that collect and enable the transmission of data—cables, connectors, patch cords, sensors, switches, and so on—must be able to withstand the harsh conditions and high-performance expectations in these environments. This is the industrial Ethernet, which can be compared to a backbone that connects all parts of a manufacturing enterprise—from the corporate office and the production floor to remote locations. These platforms provide both internet and enterprise connectivity.

IIoT platform. In IIoT, platforms are designed to deploy applications that monitor, manage, and control connected devices. IIoT platforms handle problems such as connecting and extracting data from a vast number and variety of end points, which are sometimes in inconvenient locations with spotty connectivity.

Industrial software stack. The industrial software stack is the complete set of software products and tools required to gather data from an industrial end point (a machine), extract useful information from that data, and either inform or initiate a decision on how to operate the machine differently or support other decisions on how to operate the underlying business more effectively.

Industry 4.0. Industry 4.0 is one of the names given to the current trend of automation and data exchange in manufacturing technologies, and includes cyber-physical systems, IoT, cloud computing, and cognitive computing. Industry 4.0 is commonly referred to as the Fourth Industrial Revolution and fosters what are called "smart factories." Within modularly structured smart factories, cyber-physical systems monitor physical processes, create a virtual copy of the physical world, and make decentralized decisions. Over IoT, cyber-physical systems communicate and cooperate with each other and with humans in real time, both internally and across organizational services offered and used by participants in the value chain.

Information technology (IT). IT includes any use of computers, storage, networking, or other physical devices, infrastructure, and processes to create, process, store, secure, and exchange all forms of electronic data.

Internet of Things (IoT). IoT refers to the connectivity of physical objects and devices to the internet, enabling the exchange of data. In this report, IoT refers to consumer-oriented applications, in contrast to the industrial applications that IIoT refers to.

IO-Link. IO-Link is a short-distance, bidirectional, digital, point-to-point, wired (or wireless), industrial communications networking standard used for connecting digital sensors and actuators to either a type of industrial Fieldbus or a type of industrial Ethernet. Its objective is to provide a technological platform that enables the development and use of sensors and actuators that can produce and consume enriched sets of data, which can in turn be used for economically optimizing automated industrial processes and operations.

IT-OT convergence. IT-OT convergence is the integration of IT systems with OT systems. IT systems are used for data-centric computing; OT systems monitor events, processes, and devices, and make adjustments in enterprise and industrial operations. There are three main categories of IT-OT convergence: 1) process convergence, which covers the convergence of workflows, 2) software and data convergence, which deals with putting front-office software and data to work to address OT needs, and 3) physical convergence, which includes converging or retrofitting physical devices with newer hardware to accommodate the addition of IT to traditional OT.

Low-code/no-code platforms. A low-code development platform is software that provides a development environment used to create application software through graphical user interfaces and configuration instead of traditional hand-coded computer programming. A low-code model enables developers of varied experience levels to create applications using a visual user interface in combination with model-driven logic. A no-code development platform allows programmers and nonprogrammers to create application software through graphical user interfaces and configuration instead of traditional computer programming. No-code development platforms are closely related to low-code development platforms, as both are designed to expedite the application development process.

Manufacturing execution system. A manufacturing execution system manages manufacturing operations within a factory. It receives product definitions, electronic work instructions, and equipment settings from the product life-cycle management system and order requirements from the enterprise resource planning system. It then reports production performance results and consumed materials to the enterprise resource planning system.

Manufacturing operations management (MOM) system. MOM is a methodology for viewing an end-to-end manufacturing process with the goal of optimizing efficiency. The many types of MOM systems include software for production management, performance analysis, quality, and compliance, and human-machine interfaces. Production management software provides real-time information about jobs and orders, labor and materials, machine status, and product shipments. Performance analysis software displays metrics at the machine, line, plant, and enterprise level for situational or historical analysis. Quality and compliance software is used to promote compliance with standards and specifications for operational processes and procedures. Human-machine interface software is a form of MOM software that enables operators to manage industrial and process-control machinery using a computer-based interface.

MQTT. MQTT is a modern, lightweight communication protocol, effectively allowing the connection of remote devices with a small code footprint at very low network bandwidths.

Open platform communications (OPC). OPC is the interoperability standard for the secure and reliable exchange of data in the industrial automation space and other industries. It is platform independent and ensures the seamless flow of information between devices from multiple vendors.

Operational technology (OT). OT, which is traditionally associated with manufacturing and industrial environments, includes industrial control systems such as supervisory control and data acquisition. While IT inherently covers communications as a part of its information scope, OT has not traditionally been a networked type of technology, meaning not connected to a larger network over the internet. Many devices for monitoring or adjustment were not computerized in the past, and those with computing resources generally used closed, proprietary protocols and PLCs rather than technologies that afforded full computer control.

Platform. A platform is software and hardware which may include an operating environment, storage, computing power, security, development tools, and many other common functions. Platforms are designed to support multiple, smaller business solution applications.

Product life-cycle management. Product life-cycle management is a software system that consolidates production information and facilitates the design, manufacturing, service, and disposal of resources involved in the production process.

Programmable logic controller (PLC). A PLC is a small, modular solid-state computer with customized instructions for performing a particular task. Used in industrial control systems for a wide variety of industries, PLCs have largely replaced mechanical relays, drum sequencers, and cam timers.

Supervisory control and data acquisition. Supervisory control and data acquisition is a control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level process supervision, and uses other peripheral devices, such as PLCs and discrete proportional-integral-derivative controllers, to interface with the process plant or machinery. The supervisory control and data acquisition computer system handles operator interfaces that enable monitoring and issuing of process commands, such as controller set-point changes. However, the real-time control logic or controller calculations are performed by networked modules that connect to the field sensors and actuators.

Supply-chain management software. Supply-chain management requires software tools or modules to execute supply-chain transactions, manage supplier relationships, and control associated business processes. While functionality in such systems can often be broad, they commonly include customer requirement processing, purchase order processing, sales and distribution, inventory management, goods receipt and warehouse management, and supplier management/sourcing.

Authors

Andreas Behrendt
Partner, Cologne office
Andreas_Behrendt@mckinsey.com

Enno de Boer
Partner, New Jersey office
Enno_de_Boer@mckinsey.com

Tarek Kasah
Associate Partner, Düsseldorf office
Tarek_Kasah@mckinsey.com

Bodo Koerber
Partner, Düsseldorf office
Bodo_Koerber@mckinsey.com

Niko Mohr
Partner, Düsseldorf office
Niko_Mohr@mckinsey.com

Gérard Richter
Senior Partner, Frankfurt office
Gerard_Richter@mckinsey.com

The authors wish to thank Isabel Blum, Alexander Busse, Beltir Caglar-Dayanik, Bill Corrigan, Leonides de Ocampo, Robert Feldmann, Jörg Hanebrink, Alexander Knaak, Zina Kolesova, Dennis Küsters, Prashanth Parthasarathy, Tyler Smith, Florian Surek, Joris van Niel, Zach Warren, Adrian Widmer, and Hayden Zheng for their contributions to this report.

February 2021

Designed by Visual Media Europe

www.mckinsey.com

@McKinsey
@McKinsey