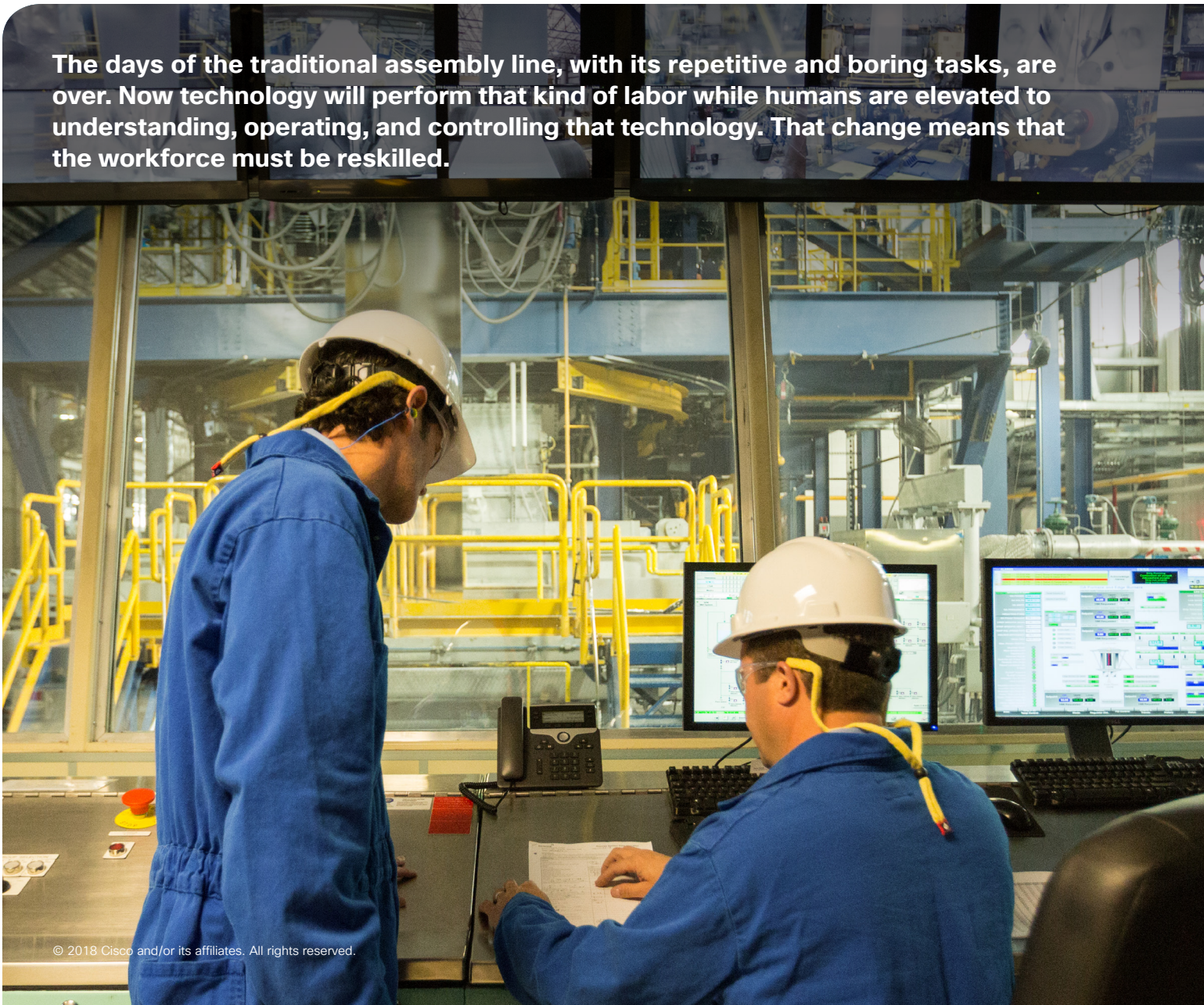
IoT Digital Transformation: Changes in Manufacturing Processes Can Boost Competitiveness

The days of the traditional assembly line, with its repetitive and boring tasks, are over. Now technology will perform that kind of labor while humans are elevated to understanding, operating, and controlling that technology. That change means that the workforce must be reskilled.



The manufacturing plant is becoming "smarter," with machines and systems that cannot only communicate with each other, but that can also act on that information.

In our previous white paper, "Prepare to Succeed with the Internet of Things," we discussed how the Internet of Things (IoT) has been brought into the industrial world. Now in this paper—the second in a series for organizational management—we discuss the production process changes necessary for digital transformation in manufacturing.

In the Industrial Internet of Things (IIoT), machines, tools, and processes that once were essentially standalone are now connected to each other and to the production system—and even to the entire company and to customers and vendors.

In other words, the manufacturing plant is entering the digital age in a significant way. It is becoming "smarter," with machines and systems that cannot only communicate with each other, but that can also act on that information.

This is not just a future fantasy. It's happening today with a growing number of industry leaders, such as GE, IBM, and Amazon Web Services, all of which are moving swiftly into IIoT. Any company that doesn't act soon will be left on the sidelines.

In fact, the automation accompanying IIoT is streamlining the manufacturing process while bringing new efficiencies and cost reductions to almost the entire system:

- Thanks to IIoT, manufacturers can efficiently produce limited runs of specialized products, and they can quickly adapt to producing new and evolving products. Thus, these companies will become more competitive and profitable.
- The days of the traditional assembly line, with its repetitive and boring tasks, are over. Now technology will perform that kind of labor while humans are elevated to understanding, operating, and controlling that technology. That change means that the workforce must be reskilled.
- In the IIoT factory, detailed maintenance records, life cycles, faults, and other machine and tool data can be stored in the cloud for immediate notification and reference, thereby preventing failures and shutdowns.
- Order processing, shipping, and delivery records can be tracked in real time, even by the customer, reducing the number of inquiries about order status.
- Automated inventory controls can transmit notifications to the purchasing department to place orders for additional supplies and materials before a critical shortage occurs.
- A cloud-based enterprise resource planning (ERP) system can greatly streamline back-office operations and processes because it is much more flexible and nimble than traditional ERP systems.
- IIoT will also catalyze an increase in the pool of qualified workers who have the initiative to train and earn certifications in these new technologies.

Many industries are rapidly connecting to IoT because of the emergent IIoT-enabled digital transformation.

IIoT will require new manufacturing systems

First, let's provide a little history. Before the transition from analog to digital in the 1950s, manufacturers deployed discrete controllers (relays, timers, and sequencers) for monitoring and combinational logical control of local field devices, such as sensors and control elements.

The many discrete controllers soon would be replaced with digital processors (that is, microcontrollers), each running autonomously while communicating over a LAN with a centralized graphic display. This became the distributed control system (DCS), the beginning of industrial networking.

Digital computing allowed programmable logic controllers (PLCs) to use flexible process controls in place of relays and timers.

The new digital supervisory control and data acquisition systems (SCADAs) consisted of a centralized server with human-machine interface (HMI). The SCADA collected data from a network of geographically distributed PLCs using industrial networking protocols for area supervision and control.

This collection of PLC, DCS, and SCADA is generally referred to as the industrial control system (ICS).

With the advent of digital computing, the graphical user interface, and networking technology, the ICS has moved from unit-based monitoring and control to plant-level supervision.

Industries recognize that running an isolated, inflexible, and proprietary process control system is not a viable business model. It makes much more business sense to adopt IT capabilities for economies of scale.

In the 1990s, the Purdue Enterprise Reference Architecture was developed for computer-integrated manufacturing. The architecture has been further developed, and an important component is the Purdue Model for Control Hierarchy, which segments devices and equipment into hierarchical functions. The model identified five key zones and six levels of operations for an ICS. It further connects the ICS (Levels 0–2) to the upper production control (Level 3) and business logistics (Level 4) operation levels.

Many industries are rapidly connecting to IoT because of the emergent IIoT-enabled digital transformation.

The ICS is deployed in a wide variety of industries because it includes many process control methods in manufacturing (including batch, discrete, and hybrid), transportation, oil and gas, mining, pulp and paper, and so on.

Let's use manufacturing as an example. Cisco works with Rockwell Automation on the Converged Plantwide Ethernet (CPwE) reference architecture, blending Open Systems Interconnection (OSI) with the six-level plant logical framework. This comprises a Rockwell Automation ICS with Cisco Ethernet (EtherNet/IP) for the connected factory while using open standards.

This convergent architecture requires OT and IT professionals to strive for an unprecedented level of collaboration.

The integration of best-in-class industry knowledge from Rockwell and Cisco provides a powerful reference architecture for manufacturing to leverage the best of IT wired and wireless technology, security, high availability, and economics. What once were vendor-specific ICS devices can now interconnect over a common network, scalable to thousands of connected devices.

Operational technology (OT) runs Levels 0-2 for process control, and IT manages Levels 3 and 4 in the enterprise domain for overall business and production control. In this way, the OT network is effectively connected with the enterprise IT network. This convergent architecture requires OT and IT professionals to strive for an unprecedented level of collaboration. Further, this shift happens both on and off the factory floor.

The CPwE implementation guide is based on the ISA99-defined plant logical framework from the Purdue Model.

Traditionally, safety systems were segmented from the ICS to provide overall control of safety events. As safety standards and protocols have evolved, it has become beneficial economically and functionally for safety devices to interoperate with Level 0 ICS devices.

EtherNet/IP enables implementation of distributed safety control within the ICS network. An independent safety zone is not considered in the CPwE design and implementation guide.

CPwE supports interconnectivity of devices and industrial protocols from various suppliers, plus interoperability between process control and manufacturing/enterprise applications, as well as real-time communications among connected things and software. In the Cell/Area Zone (EtherNet/IP traffic, real-time control, and so on), CPwE must support the network topologies required by various industrial applications. Overlay CPwE with the need for a security blanket, and we can see that the industry is facing a widening talent gap. Why? Because neither IT nor OT understand this convergence complexity. They must be upskilled to become capable IIoT engineers.

It is recommended that the converged network be a managed network. This is because a managed infrastructure leverages widely adopted IP networking technologies and protocols to support advanced features such as segmentation and VLANs, security, diagnostics, quality of service (QoS), network traffic shaping, scalability, resiliency, and high availability. In networking enterprise with industrial, we find that segmentation of Cell/Area Zone, Manufacturing Zone (site operations and control, routing, multiservice network, and so on), Demilitarized Zone (firewalls for segmentation, unified threat management, and so on), and Enterprise Zone (WAN and Internet network, data centers, and so on) replaces air gap security[1] for standalone process control systems. Therefore, deployment of the intelligent network infrastructure now requires skilled IIoT engineers.

1. An air gap is a network security measure deployed on computers to physically isolate them from unsecured networks, such as the public Internet or other unsecured local-area networks.

When your organization commits to embracing digital transformation, you will begin to see multiple benefits that will continue to increase exponentially.

Benefits will multiply exponentially

This all may seem rather complex and perhaps daunting. However, when your organization commits to embracing digital transformation, you will begin to see multiple benefits that will continue to increase exponentially. These include the following:

- **Multivendor device management–**Just as smartphones come from different vendors, so do sensors and controllers in the industrial verticals. Yet they all must communicate seamlessly. CPwE manages this interface.
- **Converged IT and OT automation network–**IIoT introduces some changes to the technology and "culture" of IT and OT engineering. This comes from the intricacies of connecting "things" over a multitude of industrial application protocols (such as ZigBee, Z-Wave, 6LoWPAN, and Bluetooth Low Energy, or BLE). If these engineers can adapt, then control and data information can be shared more broadly with the rest of the ecosystem over a converged IP communication network.
- **Operations management–**The automation network is the IP network connected to the management network for remote configuration, updates, and maintenance support. This is not something OT engineers are accustomed to. Therefore, they must transition from silo-based operations management to an integrated process for the connected ICSs. Eventually, business process operation will become an integral part of operations management, as well.
- **Data management and analytics–**Data analytics is the name of the game. Data from various sources communicating over various protocols and formats will be managed and presented in a common data format via open application programming interfaces (APIs) to analytics engines and services through data virtualization. Edge analytics and layered processing are supported via fog computing, also known as edge computing.
- **Service development and APIs–**As the focus shifts from connectivity to solutions, services will be key to digesting the collected data and driving the desired business outcomes. For example, when processes are connected throughout the system, organizations can provide personalized products and services to their customers. Or they can produce profitable small-batch runs to meet particular specifications. This means that the developer community must be nurtured and supported with open APIs and software development kits (SDKs) to innovate around vendor products.
- **Platform scalability–**When a project progresses from proof of concept to mass adoption, scalability and high availability must be planned into the system. This is the way to help ensure zero downtime, which is critical for manufacturing.
- **End-to-end security–**With IoT, security must be built in rather than tacked on to provide a holistic view of platform protection for incident detection and response.

IIoT manufacturing requires an integration of technologies for successful implementation.

- **Third-party integration—**Scalability and interoperability are key ingredients for IoT. This is necessary as the platform expands to cross-connect ecosystem partners and industries to maximize intelligent orchestration, as is done with connected transportation and smart cities.
- **Industry standards, regulations, and compliance—**From its machine-to-machine (M2M) roots, a multitude of IoT communication standards must be rationalized (IEEE 802.11ah, Z-Wave, ZigBee, 6LoWPAN, ULE, Thread, and so on). The selection should be based on requirements and best fit. In manufacturing, the popular industrial Ethernet standards include Common Industrial Protocol (CIP) and PROFINET. Then there is industry-related U.S. regulatory compliance for IoT services, such as PCI DSS, GLBA, FISMA, and HIPAA. Having these standards minimizes multiple-vendor proprietary implementations and lock-in while promoting interoperability. Regulatory compliance mitigates risk and legal liabilities.
- **Cisco-validated design and reference architecture—**The Industrial Internet Consortium (IIC) released an Industrial Internet Reference Architecture[2] outlining key security, privacy, connectivity, and interoperability considerations. Other important benefits that a reference architecture offers are device management, data management and analytics, scalability, and high availability. Cisco collaborates with industrial leaders and subject matter experts to provide customers with Cisco Validated Designs based on the IoT reference architecture.
- **The glue—**As we can see, the IoT platform is an ecosystem of technologies and contributors. Besides technical knowledge, the "magic glue" that coalesces the many platform components and functions into a solution necessitates a set of soft skills: collaboration, communications, project management, business values, and leadership. Valuable business outcomes can be derived when organizations optimize the interworking of these platform components—for example, more accurate process scheduling and materials ordering.

Technology integration can happen even during the transition

IIoT manufacturing requires an integration of technologies for successful implementation. While these technologies may continue to evolve, with IIoT they can be integrated and adapted even under changing conditions. Let's use the evolution of traffic controls in smart cities as an analogy:

- **Time-based controls—**In the past, traffic light controls were time-based, with signals changing at set intervals regardless of traffic flow. Everyone knows the frustration of waiting at an intersection for the green light when no other cars are present. This can be compared with the more proscribed manufacturing functions under the Purdue Model. They work adequately, and they accomplish their purpose. But they are not flexible or efficient.

2. Industrial Internet Consortium, Industrial Internet Reference Architecture, v1.8, January 2017.

If CEOs think that digital transformation can be challenging, they're correct. It takes bold vision and an ability to try new things, take small steps, and build on incremental success.

- **Hybrid systems–**In today's smart cities, traffic light controls are a hybrid system of timers with connected sensor inputs that react when a vehicle is detected. While a vehicle may not need to wait unnecessarily at intersections, it may still, annoyingly, have to stop at each traffic light on its route. In manufacturing, this can be compared with a facility that is undergoing a transition into the IIoT paradigm. It is not quite at its goal, but functions and processes have been instituted to transition the operation.
- **Integrated systems–**With citywide traffic analytics enabled by integrated operations, traffic flow can be better shaped, and congestion can be managed through integrated operations for situational alternate routing. The travel down the road can be much smoother with traffic-shaping analytics. For the manufacturing facility, this would be compared with full integration of IIoT. Functions and processes are now automated, tools and machines are communicating with each other and with the system, and the operation is much more efficient, flexible, and cost-effective.

Leading companies are already deep into IIoT

According to Network World,[3] many global companies are moving rapidly into IIoT. For example, GE plans to leverage IIoT by connecting manufacturing devices to the Internet through its Asset Performance Management platform. IBM is making a big push with its Watson smart products, which are planned to inject "cognitive abilities" into its IoT services.

Amazon Web Services is storing huge amounts of data and is offering powerful services to gain insight on that data, such as buyer behavior and preferences. Salesforce.com is using IoT to help marketers gain insight into their customers and prospects. AT&T is moving quickly toward connecting 10 million vehicles to its network, including fleet vehicles and shipping containers. Bosch is connecting its products to the Internet to track maintenance and to monitor devices. Cisco has carved out a whole range of IoT services, from network connectivity to management and automation. And Samsung says all its products will be IoT-ready by 2020. These are just a few of the leaders in their respective industries already making that digital transition.

If CEOs think that digital transformation can be challenging, they're correct. It takes bold vision and an ability to try new things, take small steps, and build on incremental success. But it also takes the fortitude to quickly cast aside things that don't work or that will take too much time and energy to bring to a workable stage. "Quick-to-fail" actually helps navigate investment to the path of success, evidenced by Cisco findings announced at the 2017 IoT World Forum.[4]

It requires the ability to look down the road to see not just where you're going, but also where you want to go. Aiming the company into the future

3. Gold, Jon; Network World, "Most Powerful Internet of Things Companies," February 26, 2018.
4. Cisco news release, "Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing," May 23, 2017.

Companies that don't already have a chief digital officer (CDO) must think seriously about instituting that role.

requires the ability to imagine the possibilities. And it takes understanding—that the targets will move, that more changes will come quickly, that industry leaders can rise and fall.

Gone are the days when a company can become a leader and then rest on its merits for a decade or more. Now speed, agility, and vision are necessary to remain at the top—plus an ability to adapt to changing technologies.

Disruption is at the center

Companies that don't already have a chief digital officer (CDO) must think seriously about instituting that role. A CDO should be a disruptor—someone who is willing to take chances, who has the leadership ability to persuade a team to carry out a plan, and who has the smarts to know the difference between an idea that is working and one that is not.

This person also should have the backing of the CEO, because disruption is often uncomfortable. Management may balk. Line workers may not understand what the change is about. Every day, the CDO may be facing those who say, "But we haven't done it this way before."

But that's the point. The company should be doing things that haven't been done before—so long as they are done with a clear vision and not simply as "change for the sake of change."

Earlier this year, Harvard Business Review presented an article about how CEOs can lead a digital transformation by prioritizing their goals.[5] In it, author Laurent-Pierre Baculard offered three steps, which are summarized here:

- **Define where change is needed most—**Digital technology tends to create or destroy value in four critical areas—customer engagement, digital products and services, operational performance, and preparing for disruptive new business models. It takes a clear view of the opportunities or threats in each area to determine which capabilities need the most attention and where to concentrate investment.
- **Choreograph the change—**Even the clearest digital strategy will fail if people are unprepared to embrace it. Defining where you need change is critical. But so is setting up the capabilities and processes that will enable it.
- **Empower people—**Recognize the central importance of an orchestration model for digital—prototyping, risk taking, and mobilizing the front line to push concrete initiatives. Many of today's leading digital models have been distributed throughout global organizations via "digital relays," or champions within each geography and business unit.

5. Baculard, Laurent-Pierre; Harvard Business Review, "To Lead a Digital Transformation, CEOs Must Prioritize," January 2, 2017.

Before your organization can embark successfully on its digital transformation, your management and staff must be educated and prepared for the new technologies and processes.

Details will be different for each industry

It's difficult to provide a single roadmap for various manufacturers as they head into the exciting realm of digital transformation. An automotive factory may require different technologies than a textiles producer, and a large multinational company will require a different framework than a more localized factory.

For some, digital transformation will require retooling an entire assembly line for automation. For others, it may involve radio frequency identification (RFID) tag tracking for shipping, receiving, and inventory control. And for still others, it may require expanding the data center, or rewriting technical policies and procedures, or expanding the parameters of the digital security system. In fact, some companies may find that it will require all this and more.

For all organizations, it will involve retraining personnel—assembly workers, accounting teams, records administrators, security experts, IT staff, and even C-level management. Nearly everyone on the team will be affected, and they must understand and become proficient with new and ever-changing technologies and processes.

Moreover, the management approach to disruption varies from industry to industry. Some industries are more conservative, less risk-tolerant, and may even be reactive to changes. But transformation is necessary at the leadership level for organizations to stay competitive.

Cisco is here to help

Before your organization can embark successfully on its digital transformation, your management and staff must be educated and prepared for the new technologies and processes. Cisco offers appropriate industry-respected courses in the necessary topics to address the IoT-enabled digital transformation for your team:

- "Managing Industrial Networks with Cisco Networking Technologies" (IMINS), an instructor-led course that leads to Cisco Industrial Networking Specialist certification.

  IMINS is a lab-based course for those who need the foundational skills necessary to manage and administer networked industrial control systems. It is especially appropriate for plant administrators, control system engineers, and traditional network engineers who must understand the networking technologies necessary in connected plants and enterprises. This course also helps participants prepare to take the exam that is required to earn the Cisco Industrial Networking Specialist certification.

  The IMINS course is job role-specific, enabling participants to become competent in configuring, maintaining, and troubleshooting industrial network systems while helping to ensure network availability and reliability. It also addresses Internet security throughout the company. Participants are exposed to multiple industrial network technologies as well as products from Cisco and other industrial suppliers, including Rockwell Automation.

Do not let the complexity of new challenges prevent you from joining the digital transformation. It will be essential to your survival in a changing landscape.

- "Managing Industrial Networks for Manufacturing with Cisco Technologies" (IMINS2), an e-learning course that leads to Cisco CCNA Industrial certification (with an instructor-led version of the course also available)

  The IMINS2 course is designed for IT and OT professionals, teaching best practices used in security and wireless technologies for industrial networks. It caters to plant administrators, control systems engineers, and traditional network engineers in the oil and gas, process control, and manufacturing industries who are involved with the convergence of IT and industrial networks. It prepares students for the exam that is required to qualify for the Cisco CCNA Industrial certification.

  IMINS2 is also job role–specific, enabling participants to become competent in configuring, maintaining, and troubleshooting industry-standard network protocols as well as wireless and security technologies. It also covers multiple industrial network technologies. Participants learn how to make full use of current infrastructures while developing a converged platform with the flexibility to support future business outcomes.

For more information, visit Cisco's Internet of Things Training page.

Now is the time to get started

Considering all these essential changes to the manufacturing process, it is not too early to get started. Do not let the complexity of the new challenges prevent you from joining the digital transformation. It will be essential to your survival in a changing landscape, where you will be expected to adapt or perish.

Use the industry leaders as your role models. Investigate what they are doing, and see how you can apply it to your own organization. And understand that once you begin this foundational change, you also must start educating your people so they can support these processes in the best possible way.