industrial internet
CONSORTIUM

Digital Transformation in Industry White Paper

An Industrial Internet Consortium White Paper

Version 1.0

2020-07-29

CONTENTS

FIGURES

TABLES

Digital transformation ("DX") is a general term used in several market spaces and domains, for example:

- in the consumer space, disruptive technologies have transformed how media content is delivered to consumers (for example, Netflix and Uber),
- in business, mobile payment applications have transformed the way individuals and corporations consume banking services and
- in industry, disruptive technologies are transforming how companies operate, service, and maintain equipment.

These DX domains are all based on internet connectedness, consumer-to-consumer, service consumer-to-service providers, consumer-to-business, and systems-to-machines and other physical things. The arrows in figure 0-1 suggest a timeline of when things started for these types of digital transformation. The ends of the arrows represent today. The thicknesses are indications of market impact.

Figure 0-1: Digital Transformation in Industry–source IIC

Disruptive technologies are transforming industries into digital industries, a "caterpillar-to-butterfly" journey, which in some cases is a "do-or-die" proposition. This transformation can present major challenges, outside of normal business models and technological concerns, for example, compliance with security and regulatory pressures.

We provide a general overview of *digital transformation* (DX) in industry and the types of better outcomes that organizations seek when they embark on DX journeys. We also highlight:

- the business factors (section 1),
- key technologies (section 2) and
- trustworthiness factors (section 3) that underpin these journeys.

The paper targets business managers who are involved in setting the digital transformation strategy and journey for an organization, and technology managers who need to identify and assess how technologies can be leveraged to facilitate the DX journey. Finally, we target risk, security and safety managers responsible for implementing protection and mitigation strategies to minimize the impact of disruptions, attacks, errors and faults along the journey.

1 IIC Approach to Digital Transformation

The Industrial Internet Consortium (IIC)[1] is transforming business and society by accelerating the Industrial Internet of Things[2] (IIoT[3]). Since its founding, IoT has matured, with an explosion of use cases and applications that continue to transform business, industry, and society.

With the continued maturation of IoT, there is a growing realization that it is one of several sets[4] of technologies that are driving the transformation of business, industry, and society. The IIC has thus widened its focus to include this broader set of technologies and how they empower this digital transformation in industry.

The transformation of industries into digital industries can present major challenges in terms of security and regulatory pressures. Digital transformation is primarily a business objective. It is the innovative and principled application of digital technologies, and the strategic realignment of the organization towards the improvement of business models, industrial models, and processes and ultimately the creation of entirely new ones.

Definition: Digital transformation in industry leverages connected things to transform processes and operations to produce better outcomes (figure 1-1).

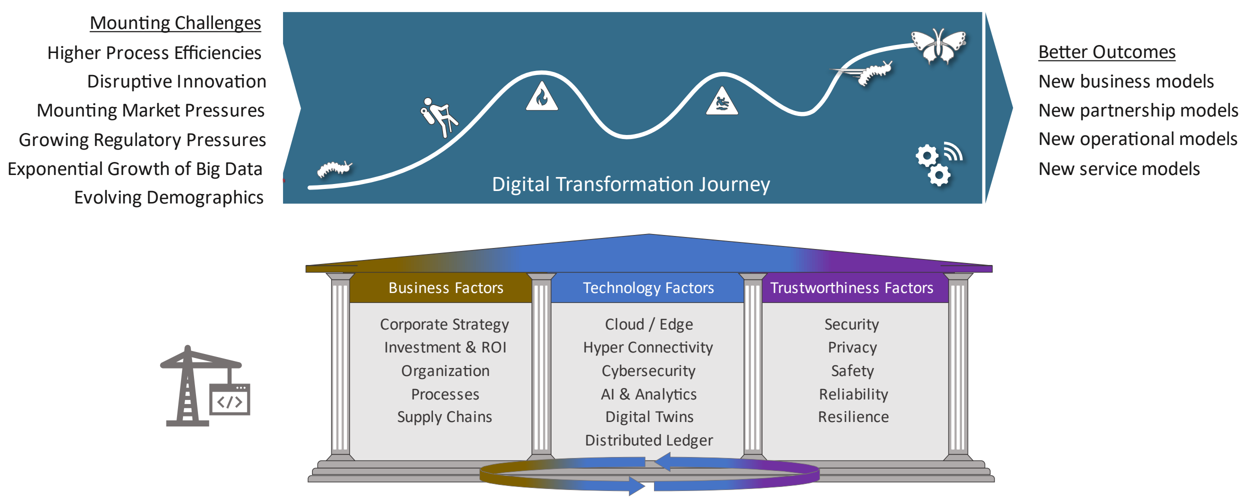

Figure 1-1: Digital Transformation Journey–source IIC

---

1 *https://www.iiconsortium.org/*
2 *https://www.iiconsortium.org/vocab/IIC_Vocab_Technical_Report_2.2.pdf*
3 In this paper the terms IIoT and IoT are used interchangeably to refer to Industrial IoT.
4 Refer to section 2 for details.

A distinguishing aspect of digital transformation in industry, as opposed to digital transformation for consumers and in wider business, is the convergence of Information Technology (IT) and Operational Technology (OT). In DX in industry, the innovative use of sensor-driven data and data-driven actuators affect people, business, operation, and the physical environment and empower the creation of better business outcomes.

We focus on digital transformation from the perspective of filling the gap between strategy and processes of innovation, and new technologies that enable more complex interaction of IT and OT technologies. The IIC's mission. of "delivering a trustworthy IIoT in which the world's systems and devices are securely connected and controlled to deliver transformational outcomes", is closely associated with the innovation projects of member companies. The IIC is well positioned to fill the gap between industrial transformation strategy and processes of innovation and also the gap between the process of innovation and resources of firms.

Digital transformation in industry should encompass innovation processes when integrating IT and OT. This is based on the view that DX can best be achieved by adopting new business models. This includes new value propositions made possible by accumulating successes in innovation and by reducing the conflicts between these new and incumbent processes, and other parts of management systems. This is done by changing the designs of management systems.

Before delving into the details of digital transformation, we examine three related terms that are sometimes used interchangeably:

- digitization,
- digitalization and
- digital transformation.

Figure 1-2 below illustrates the differences between these terms and their progressive nature:

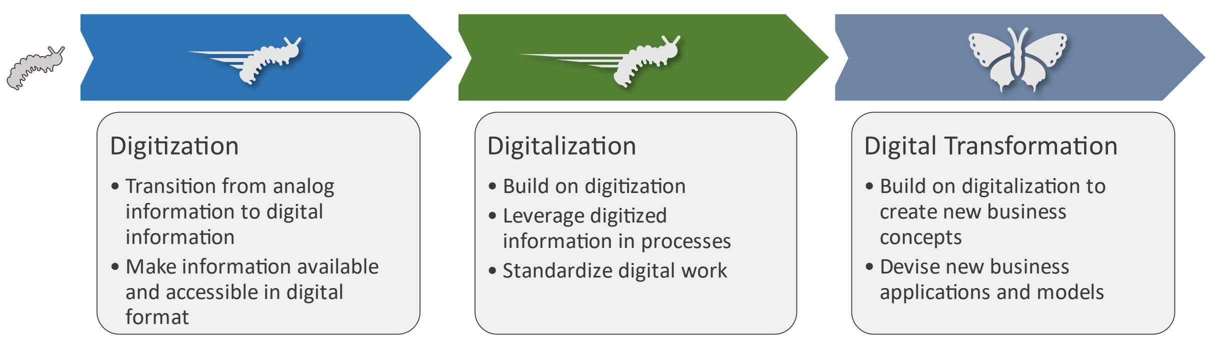

Figure 1-2: Digitization, Digitalization and Digital Transformation–source IIC

<u>Important:</u> Although we focus on digital transformation, some industrial organizations use the term to encompass digitization and digitalization. These organizations may be focused on digitizing and improving their process and operational efficiencies only or it may be a first phase of a gradual progression towards digital transformation.

The driving force for DX is often *market pressure*: competition, or the threat of competition. If one participant in a market successfully implements a digitally transformative project, then competitors in that market will feel compelled also to transform—or risk losing competitiveness and market share.

The routes by which such competitive advantages come about range from *higher process efficiencies* enabling lower pricing to customers through to *disruptive innovation* and the implementation of a new customer proposition in the marketplace that is significantly different from existing propositions.

Regulatory pressures have historically been a significant driver of business transformation, and this will increase in the wake of COVID-19, with an increased focus on 'safe' working practices and social distancing.

Beyond these driving forces are a range of indirect forces that may prompt enterprises to rethink how they do business. For instance, *evolving demographics* and an aging population may force a healthcare insurance provider to rethink how their services are provided to older clients.

There are network effects at play too. The simple availability of new technologies and techniques means that enterprises can consider transforming their businesses in ways that, until now, have not been possible. One of the most significant considerations in this context is the quantity, quality and timeliness of information and the *exponential growth of big data*.

In all, the motivations for deploying digitally transformative solutions are diverse, but they share a need (or desire) to do business in a new and better way.

Digital transformation initiatives fall into three categories:

- those encompassing new business models and that affect both enterprise value propositions and efficiency,
- those that affect enterprise operations and support activities but not customer experience and
- those that affect customer experience, but not operational efficiency.

New business models entail an enterprise transforming to offer a substantially changed service to end users, often associated with new ways of charging for services. A classic example is a vendor of hardware assets offering those same assets as a service. Such changes often involve far-reaching changes to the operating model of an enterprise, including the need to instantiate new kinds of ongoing client support capabilities such as customer service capabilities, recurring billing capabilities, field support capabilities and enforceable and auditable protocols for service and maintenance compliance.

Some digital transformation projects focus on either *new partnership models* or *new operational models* and leave the value proposition of the enterprise deploying the solution relatively unchanged, focusing primarily on increasing the efficiency (or reducing the cost, or risk) of providing products and services to end users. An example is an airline changing the way that spare parts are purchased to provide additional transparency of stock levels through the supply chain and increase efficiency. Such a project does not affect the airline's overall proposition to its passengers and is instead a 'behind the scenes' change. A project of this kind could rely on distributed ledger technologies to allow for new levels of sharing information between parties in the supply chain for any parts and reduce the service and maintenance costs of aircraft.

A final category of digital transformation focusses on changing the customer experience in the absence of or in addition to other changes. This kind of project tends to focus on generating *new service revenues* or providing *new services* to customers, particularly field services. Such projects leave the overall existing operations of an enterprise relatively unchanged, while overlaying a new capability for an improved overall customer proposition. If a company deploying such a service were to take the next step to guarantee the performance of an asset, then it would inevitably impact both support operations and the end user proposition.

2 Key Technologies Underpinning DX

Digital transformation is a journey from the Mounting Challenges to the Better Outcomes (figure 1-1). The journey is underpinned by three factors: business, technology and trustworthiness.

Industrial IoT is about connecting "things" to a network and capturing operational and contextual data (potentially big data) about these "things" with the purpose of controlling them and optimizing their operation. This opens the door to innovative use of a wide range of emerging (and some well-established) technologies that together enable the digital transformation sought.

The following sections provide an overview of some of these emerging technologies[1] and their key usage scenarios within a DX context.

2.1 Cloud/Edge

DX Technology: Edge
Edge technologies bring processing intelligence closer to data sources, allowing (near-)real-time responsiveness and improved functionality in situations where local devices may not be continuously connected to data center resources.

[1] The list of innovations and advancements in technology that can affect digital transformation is too long to be covered here, and includes innovations around sensors and actuators, advancements in nanotechnology (nano robots, supercapacitor batteries, etc.)

DX Technology: Edge
Key usage scenarios: • Edge computing can enable improved solution performance, including more responsive applications, improved robustness and reliability and autonomous operation. • Storing and processing data nearer to data sources can help with regulatory compliance, including privacy and security. • Redaction at the edge can reduce connectivity, data migration and bandwidth costs associated with sending data to the data center.
Relevant IIC publications: • *Journal of Innovation: September 2017* • *Introduction to Edge Computing in IIoT (White Paper)* • *The Edge Computing Advantage (White Paper)*
Opportunities for the IIC: • Develop guidelines for how artificial intelligence applications can be optimized across data center and edge assets. • Investigate how multi-access edge computing (MEC) can be used to support industrial users, including the limitations of MEC solutions. • Develop guidelines for how local processing capabilities can be most effectively shared between local edge devices, deployed in a solution.

Table 2-1: Edge Technology

2.2 Hyper-Connectivity

DX Technology: Hyper-Connectivity
Hyper-connectivity describes an environment of ubiquitous connectivity, often with specialized functionality adapted to the demands of a particular application. Key technologies from an IIC perspective include 5G Ultra-Reliable Low Latency Communications (URLLC), Enhanced Mobile Broadband (EMB) and Massive Machine Type Communications (mMTC) in both public and private networks and alternative Low Power Wide Area networks (LPWA) technologies. Additional technologies include mesh networks, high altitude low orbit (HALO) platforms and evolving Wi-Fi standards.
Key usage scenarios: • 5G URLLC allows wireless networks to be deployed to support critical and low latency communications needs, such as wireless emergency-stop functionality for industrial machines.

DX Technology: Hyper-Connectivity
• The interworking of public and private 5G networks will allow for applications that work seamlessly when roaming between campus and off-campus locations. • LPWA technologies will enable new IIoT applications by decreasing the cost of wide-area connectivity and allowing for extended battery life.
Relevant IIC publications: • *Industrial Networking Enabling IIoT Communication (White Paper)*
Opportunities for the IIC: • Determine how best to interwork public and private 5G networks, including support for edge computing applications. • Develop guidelines for how to develop power-efficient applications to maximize the potential of NB-IoT. • Develop guidelines to identify the most suitable LPWA technologies in different scenarios. • Profile the strengths and weaknesses of different connectivity alternatives in different circumstances.

Table 2-2: Hyper Connectivity

2.3 Data Security

DX Technology: Data Security
Protecting sensitive data created, stored, and consumed by IIoT technology and applications is one of the foundations of trustworthy[1] IIoT systems, itself one of the underpinnings of DX. Data security is a property of being protected from unintended or unauthorized access, change or destruction ensuring availability, integrity, and confidentiality. It falls under the broader umbrella of data protection and encompasses several adjacent and overlapping domains, such as data security, data integrity and data privacy. Data security covers a wide range of protection mechanisms such as key management, root of trust, authentication, access control and audit & monitoring.
Key usage scenarios: • Allows organizations to protect data-in-motion, data-at-rest and data-in-use to prevent unauthorized access to such data and tampering with such data.

[1] Refer to section 3 Digital Transformation and Trustworthiness for further details.

DX Technology: Data Security
• Plays a central role in the enablement of IoT trustworthiness and its characteristics: privacy, reliability, resilience, and safety. • Prevents unauthorized tampering with data that could lead to safety incidents. The IEC 61508[1] standard applies to functional safety for electronic controllers used in industrial IoT systems. Tampering with the system commands sent to such systems that determine how the operating state of the system would change, can push the system into a dangerous state. • Security can also affect the safety of systems that rely on software for safe operation. Thus, this software must be protected throughout its lifecycle.[2]
Relevant IIC publications: • *IoT Security Maturity Model (White Paper)* • *Industrial Internet Vocabulary (Technical Report)* • *Data Protection Best Practices (White Paper)* • *IoT Security Maturity Model (SMM): Practitioner's Guide (Technical Report)* • *Software Trustworthiness Best Practices (White Paper)*
Opportunities for the IIC: • Develop guidelines for how the IIC Security Maturity Model can be used to ensure the DX journey is not affected by security risks and threats. • Develop guidelines for how security can be used to ensure compliance with data privacy requirements.

Table 2-3: Data Security

2.4 AI & Analytics

DX Technology: Artificial Intelligence and Analytics
The Merriam-Webster Dictionary defines Artificial Intelligence (AI[3]) as "a branch of computer science dealing with the simulation of intelligent behavior in computers" and as "the capability of a machine to imitate intelligent human behavior".

[1] *http://www.iloencyclopaedia.org/part-viii-12633/safety-applications/94-58-safety-applications/electrical-electronic-and-programmable-electronic-safety-related-control-systems*

[2] As-written, in-delivery, at-rest, in-operation, end-of-support, and end-of-life.

[3] *https://www.merriam-webster.com/dictionary/artificial%20intelligence*

DX Technology: Artificial Intelligence and Analytics
AI and analytics provide an enhanced ability to understand and learn from data; information from IIoT systems provide a plethora of data that can be broken down and analyzed using AI algorithms, allowing organizations to make more informed decisions.
Key usage scenarios: • The capabilities provided by AI lend themselves to convergence with other emerging technologies in the pursuit of automated trust, immersive interfaces, hyperconnected networks and working autonomy. • AI can provide accelerated feedback from IIoT field data for improvements in operational processes and best practices. • Advanced analytics can allow organizations to find insights in extremely large sets of data (i.e., big data), providing increased quality and accountability. • AI algorithms can "learn" from previous experiences and adjust real-time to the environment. • Improved feedback loops from IIoT systems can allow for increased safety measures and higher overall quality.
Relevant IIC publications: • *Industrial Internet of Things Analytics Framework (Technical Report)* • *Industrial Analytics: The Engine Driving the IIoT Revolution (White Paper)*
Opportunities for the IIC: • Gain understanding of ethical decision-making during the implementation of AI in IIoT. • Research how risks, controls and the auditability of AI and analytics can be monitored and controlled as they relate to IIoT. • Develop frameworks to provide guidance and assistance in the development, documentation, communication, and deployment of AI in IIoT. • Establish how best to operationalize AI to ensure it works 24/7 across functions and business units in coordination with other emerging technologies such as blockchain and extended reality.

Table 2-4: Artificial Intelligence and Analytics

2.5 Digital Twins

DX Technology: Digital Twin
A digital twin (DT) is "a digital representation of a real-world entity or system",[1] including attributes and behaviors, sufficient to meet the requirements of a set of use cases. The entity in the definition of the digital representation is typically an asset, process or system. Digital twin information covers combinations of various data categories, such as: • physics-based models and data, • analytical models and data, • time-series data and historians, • transactional data, • master data, • visual models and • computations.
Key usage scenarios: • Manufacturing: help with predictive maintenance, optimize operational efficiencies, and define asset maintenance strategies. • Energy & utilities: optimize operation in real-time and conduct real-time computations on quality parameters. • Oil & Gas: subsurface well monitoring starting from the drilling stage to production, maintenance, and abandonment stages. Enables assessment of cost saving strategies and optimization of operation. • Mining: processing asset health data to optimize decisions on maintenance. • Process Automation: monitor relevant aspects of product status and assist with detection of product quality issues.
Relevant IIC publications: • *Digital Twins for Industrial Applications (White Paper)* • *Journal of Innovation: November 2019*
Opportunities for the IIC: • Investigate opportunities for interoperability between different digital twins as well as between digital twins and IoT systems. • Work with industry consortia and standards-setting groups to define best practices for interoperability between digital twins and IIoT.

[1] Gartner: *https://www.gartner.com/en/information-technology/glossary/digital-twin*

DX Technology: Digital Twin
• Investigate empowering role of digital twins in DX in Industry. • Liaise with the Digital Twin Consortium[1] (DTC) to ensure open channels for information exchange and collaboration between the IIC and DTC.

Table 2-5: Digital Twin

2.6 Distributed Ledger

DX Technology: Distributed Ledger Technology
Distributed ledger technology (DLT) provides a trusted, immutable ledger on which organizations can transmit and store valuable information based on internal operations or interactions with the organization's environment, including IIoT devices.
Key usage scenarios: • DLT is a shared ledger, meaning that each organization in a supply chain can always view the most up-to-date version of the ledger with full confidence that no reconciliations will need to be made with other organizations in the supply chain. • DLT complements IoT by ensuring that IoT data flows and transactions are secured and shared across an ecosystem of participants, automating trust within the DLT environment. In coordination with IoT and AI, DLT can validate the authenticity of data, verify identities, and enable secure, multi-party transactions. • Information in DLT is considered tamper-resistant,[2] this implies that the undetected alteration of data within the ledger is nearly impossible. Permissions to view data within the ledger, as well as the ledger itself, can be customized to each situation.
Relevant IIC publications: • *Distributed Ledgers in IIoT* • *Implementation Aspect: IIoT and Blockchain*
Opportunities for the IIC: • Investigate opportunities for interoperability between different distributed ledgers as well as between DLT and IoT systems. • Work with industry consortiums and standards-setting groups to define best practices for interoperability between DLT and IIoT.

[1] *https://www.digitaltwinconsortium.org*

[2] Advances in quantum computing can weaken the effectiveness of encryption mechanisms.

DX Technology: Distributed Ledger Technology
• Research best practices to balance decentralization, security and scalability as they apply to DLT in IIoT.

Table 2-6: Distributed Ledger

2.7 Human-Machine Interface

DX Technology: Human Machine Interface
Human-machine interfaces (HMIs) are combined hardware and software components that enable humans to interact with machines by inputting information to trigger outputs; they come in many forms, from simple buttons to complex graphical displays. Here, HMI refers to novel interfaces that have yet to become mainstream in industrial settings—such as augmented reality (AR) displays in which a person's physical environment is enhanced with a visual or audio "overlay," or virtual reality (VR) headsets that enable humans to immerse themselves completely in computer-generated environments.

Key usage scenarios:
• AR and VR can provide effective and cost-efficient job and soft-skills training.
  o AR can enhance learning by providing users with additional tools (e.g., overlay of blueprints, workflows or checklists) or communications (e.g., voice and video connectivity to remote experts) to help them complete their tasks.
  o VR simulations can enable learners to practice both tactical and soft skills until they are mastered.
• Digital twins of objects, manufacturing floors, entire factories or construction sites can be created using real-time data and imagery collected by IoT devices and mixed reality (XR) technologies. This enables activities like remote quality assurance or monitoring.
• AR imagery constructed from real-time data from IoT devices can inform business strategy and decision making (e.g., civic planning, law enforcement and crisis management).

Relevant IIC publications: • *Intelligent Realities for Workers Using Augmented Reality, Virtual Reality and Beyond (Journal of Innovation)* • *Artificial and Human Intelligence with Digital Twins (Journal of Innovation)* • *The Digital Transformation of Workers' Realities (Webinar)*

DX Technology: Human Machine Interface
Opportunities for the IIC: • Develop controls and best practices for maintaining security and trust related to IoT-XR devices and equipment. • Research how IIoT and XR can converge to provide value in business settings. • Develop thought leadership about how autonomous IIoT devices can generate additional value through well-designed HMI.

Table 2-7: Human-Machine Interface

2.8 Additive Manufacturing

DX Technology: Additive Manufacturing[1]
Additive manufacturing technology changes the way things are made by turning a digital three-dimensional design into a physical object by adding layers of material successively. Raw materials are typically plastics and other polymers, metals or ceramics and may be in the form of a liquid, powder or a sheet.
Key usage scenarios: • Economical production of mass personalized products enabled by extreme flexibility of customization of manufactured goods. • Manufacturing complex parts in a single process reduces manufacturing cost, improves quality, and simplifies supply chains (by reducing the number of components). Through innovation, manufacturing in a single process can also lead to products with complex designs that are impossible to produce using traditional methods. • 'Hybrid manufacturing' combines automated machines with additive manufacturing: e.g. tool production lines with robots and 3D printers together. • Multi-modal factory that can produce a diverse range of products, going beyond a boundary of an industry: e.g. additive production lines for automobile components that can produce a medical device. • Additive manufacturing for faster development processes integrated with manufacturing through directly making a physical object as a physical representation of a virtual design of digital twin in real time. • Usage item: prototypes, models and tools, components, jig and fixtures. • Applied industries: automotive, aerospace, defense, medical devices, jewelry casting and buildings, batteries, transistors, and LEDs.

[1] Prepared in collaboration with Ilyong Jung (GE additive Korea).

DX Technology: Additive Manufacturing[1]
Relevant IIC publications: • N/A
Opportunities for the IIC: • User industry driven thought leadership or test beds on next generation factory driving digital transformation of user firms: some relevance with Smart Factory Web and Automated Negotiation test beds. • Interoperability of additive manufacturing with security and IoT enabled manufacturing models. • Test beds or test drives or challenges utilizing additive manufacturing platforms to ensure interoperability. • Develop frameworks for management of IP in a distributed additive manufacturing context. • Develop guidelines for type-approval for additive manufactured objects.

Table 2-8: Additive Manufacturing

2.9 Data Sharing

DX Technology: Data Sharing
Data sharing is the ability to share IoT production and operational data across ecosystems and supply chain partners. The data may be also monetized with third parties. Data sharing can sometimes be the main driver for an IoT project. The sharing of IoT data must be done in compliance with mandatory obligations (legal and regulatory),[1] and in accordance with data protection requirements: privacy, confidentiality, IP, ownership, best practices, etc., as applied to data-at-rest, data-in-motion and data-in-use. The reasons for sharing of data across an ecosystem may be vary. Data may have: • intrinsic value that can be monetized, • research value and • historical value.

[1] Example Privacy, such as GDPR (EU) and CCPA (California)

DX Technology: Data Sharing
Key usage scenarios: • Smart Cities: share infrastructure data and traffic data across the city ecosystem (smart city exchanges). • Oil & Gas: share operational data across entities in the supply chain. • Manufacturing: share equipment operational and maintenance data with OEMs and operators.
Relevant IIC publications: • *Data Protection Best Practices (White Paper)* • *IoT Security Maturity Model (SMM): Practitioner's Guide (Technical Report)*
Opportunities for the IIC: • Develop guidelines for how to develop data sharing policies across an ecosystem. • Develop guidelines for how security can be leveraged to ensure compliance with data privacy (and data sharing) requirements. • Develop frameworks and protocols for the documentation of shared data, so that data can be interpreted by relevant parties in context. Liaise with the Digital Twin Consortium on this topic.

Table 2-9: Data Sharing

2.10 IIoT

DX Technology: IIoT
IIoT is a core technology in the fourth industrial revolution. It refers to the extension and use of sensor-driven internet of things to non-consumer applications (see below). IIoT systems connect and integrate the edge with enterprise systems, business processes and analytics.
Key usage scenarios: • Smart manufacturing systems that optimize production and minimize unplanned shutdowns through predictive maintenance. • Medical: connected medical devices, remote patient monitoring, cooperation between healthcare providers, etc. • Smart infrastructure: mobilize, monitor, and manage operation of utilities, gas, water, roads, buildings, power grids, etc. • Intelligent transportation systems: package logistics (air, sea, land), autonomous vehicles, internet of logistics, navigation, traffic management, public transport management, pay-as-you-drive insurance and parking, etc.

DX Technology: IIoT
Relevant IIC publications: • *Common Logical Data Model: Basis for Global ITS Innovation (Journal of Innovation)* • *Creating the Internet of Logistics (Journal of Innovation)*
Opportunities for the IIC: • Investigate and define opportunities for interoperability between different connected systems (potentially use case dependent). • Work with industry consortia and standards-setting groups to define best practices for such interoperability. • Investigate impact of ITS on the digital transformation of smart cities.

Table 2-10: IIoT

2.11 Autonomous Robotic Systems

DX Technology: Autonomous Robotic Systems
Autonomous robotic systems enhance human productivity in areas ranging from autonomous vehicles to unmanned drones and from manufacturing robotics. It allows a device to perform its tasks without requiring human control or oversight. Autonomous robotic systems are particularly beneficial in situations that require the remote operation of devices in real-time,[1] e.g. for protecting human worker safety or avoiding hash or hazardous work environment, or applications that require greater speed and precision than humans can provide.
Key usage scenarios: • Transportation, including autonomous vehicles and other passenger vehicles. • Automated distribution, delivery, and warehousing. • Unmanned Aerial Vehicles (UAVs) used in multiple deployment scenarios, including site and asset surveying. • Manufacturing and production line processing robots. • Automated operations in agriculture. • Precision robotics in healthcare
Relevant IIC publications: • N/A

[1] Example: dangerous locations.

DX Technology: Autonomous Robotic Systems
Opportunities for the IIC: • Define the landscape of emerging autonomous robotic systems. • Establish how, and in what contexts, autonomous robotic systems can benefit industry. • Analyze trustworthiness in the context of autonomous robotic systems and develop a mapping between trustworthiness in the context of an automated system and existing IIoT frameworks.

Table 2-11: Autonomous Robotic Systems

2.12 Innovation at the IT/OT Boundary

DX Technology: Innovation at the IT/OT Boundary
The boundary between the digital and physical world is delineated by IoT device—actuators that can change properties in the physical world in response of information and sensors that observe properties in the physical world and convert them into information. Innovations around sensors and actuators enhance the usage of existing operational technology or provides new purposes and markets. Core innovations are: • Sensors on a single chip including wired or wireless digital communication for miniaturized usage.[1] • Sensors with wireless digital communication, taking the complete power supply via a stamp-sized antenna from existing Wi-Fi and cell phone signals, replacing "dumb" passive RFID tags.[2] • Single-chip sensor cameras and microphones receiving and locally processing complex pictures and sound pattern instead just single signals to detect specific analog status variations.[3] • Micromechanical actuators permit executions in the physical world, direct connected with wired or wireless digital communication.[4]

[1] Multidisciplinary Digital Publishing Institute (MDPI), "sensors", special issue "on-chip sensors", https://www.mdpi.com/journal/sensors/special_issues/on-chip-sensors

[2] A non-battery Bluetooth solution is developed by Wiliot, *https://www.wiliot.com/*

[3] AT&T replaces IoT sensors with cameras, *https://enterpriseiotinsights.com/20171102/news/att-sees-video-replacing-lower-bandwidth-iot-traffic-tag4*

[4] Technology Brief 15 Micromechanical Sensors and Actuators, *http://cad.eecs.umich.edu/techbriefs/tb15.pdf*

DX Technology: Innovation at the IT/OT Boundary
• A new generation of industrial machines are being built as Cyber-Physical Systems (CPS), in which computational capabilities and physical capabilities are co-designed, co-tested and co-verified, and co-manufactured so that these capabilities are fused together by-design, rather than the conventional approach by which computational capabilities are more or less an after-thought add-on to the physical machines. CPS has unprecedented ability to control, monitor, adapt, enhance, extend and upgrade the capability of the machines by software. CPS fuses the digital and physical world and blurs the boundary between them.
Key usage scenarios: • Sensors and actuators implanted into humans and animals to detect sickness or replace damaged organs, like pacemakers but in greater variety. • Sensors and actuators with wireless communication on movable parts, for example to detect and correct degradation in gears or hydraulic systems, like tire-pressure warning systems in today's cars, but in greater variety.
Relevant IIC publications: • N/A
Opportunities for the IIC: • Define the landscape of innovation at the edge, a unique aspect of digital transformation in industrial systems. • Follow inventions in research centers and the development of products by startup companies. • Analyze the effect of edge innovation on trustworthiness in the context of automated systems and existing IIoT frameworks.

Table 2-12: Innovation at the IT/OT Boundary

2.13 Micropower Generation for IIoT End Devices - Energy Harvesting

DX Technology: Micropower Generation-Energy Harvesting
Incorporating wireless technology into IIoT solutions results in highly distributed solutions where some components may be in remote areas that are physically inaccessible, or hazardous. IoT devices may be connected to movable parts[1] that cannot have wired power supply.

[1] An example is a pressure sensor in a car tire–any wired power supply is not possible.

DX Technology: Micropower Generation-Energy Harvesting
Batteries have several downsides. The lifetime is always limited, especially with traditional batteries self-discharging over time, and, with chemical liquid processes, a guaranteed lifetime is hard to ensure. Rechargeable batteries can be refilled via environment power from sources such as solar cells, wind or heat, but again due to chemical liquid processes, the number of guaranteed charging cycles is hard to predict. Core Innovations are: • Solid-state batteries without liquids have a higher and better predicted lifetime or number of charging cycles.[1] • High-density electrical capacitors have a higher number of predicted charging cycles.[2] • Energy harvesting from Wi-Fi and cell phone signals via antenna can replace batteries in some cases.[3] • Bioelectrical processes that create energy from microorganisms.[4]
Key usage scenarios: • Pipelines: power for remote sensors and actuators. • Smart Cities: solar panels for smart light poles. • Transportation: generate power from wasted engine heat to improve efficiency. • Building and Structures: detecting damage on concrete and steel by embedded sensors. • Medical: power for body-embedded devices (including sensors) in Wireless Body Area Networks (WBAN) beyond what batteries can provide in autonomy and power density. • Devices on movable parts to detect status changes around damage, degradation, cracks etc.
Relevant IIC publications: • N/A
Opportunities for the IIC: • Define the landscape of new emerging micropower generation technologies. • Establish how and in what contexts, micropower generation technologies can benefit industry.

1 *https://en.wikipedia.org/wiki/Solid-state_battery*

2 *https://www.arrow.com/en/research-and-events/articles/supercapacitor-vs-battery-ultracapacitor-pros-and-cons*

3 A non-battery Bluetooth solution is developed by Wiliot, *https://www.wiliot.com/*

4 *https://www.sciencedirect.com/topics/agricultural-and-biological-sciences/bioelectricity*

DX Technology: Micropower Generation-Energy Harvesting
• Analyze the impact of micropower generation technologies on the trustworthiness of automated systems and existing IIoT frameworks (especially regarding reliability, resilience and safety).

Table 2-13: Micropower Generation–Energy Harvesting

2.14 SERVITIZATION

DX Technology: Servitization
Servitization is not a new technology, rather it is a new and fast-emerging application of other technologies discussed in this section. Most critically, it relies on IoT and Hyperconnectivity, but also often Artificial Intelligence and Data Sharing. It includes a range of concepts related to supplying hardware as a service so that end users may not need to purchase the servitized equipment or may benefit from associated services from the equipment provider. Often servitization is implemented as part of a pay-as-you-go commercial model, often including pre-emptive maintenance and with performance commitments underwritten by a supplier.
Key usage scenarios: • Charging end users for equipment (and associated consumables) on the basis of usage. • Remote and pre-emptive maintenance of equipment. • Remote sale and activation of enhanced capabilities through software updates, or software configuration changes. • 'Outcome as a service', where companies sell a certain result rather than the equipment to achieve that result.
Relevant IIC publications: • N/A
Opportunities for the IIC: • Develop a framework for analysis of the benefits of servitization from a manufacturer perspective, and also from an end user perspective. • Develop guidelines to establish the equipment types that will most benefit from servitization. • Establish frameworks for assignment of maintenance responsibilities for servitized equipment between end users and suppliers, including considerations of tools (such as AI) that may support shared maintenance support.

DX Technology: Servitization
• Liaise with the Digital Twin Consortium (DTC) to ensure alignment between the needs of servitization and ongoing DTC work. • Analyze the commercial implications of servitization including tax, financing, insurance, and risk management and also the impact on secondary markets for equipment (and parts).

Table 2-14: Servitization

2.15 Technical Platforms for New Business Models and Payment Methods

DX Technology: Technical Platforms for New Business Models and Payment Models
Traditionally industrial components are sold as physical goods before their usage. But by connecting such components to the internet, the component provider can track component usage exactly. This permits business and payment models for such components similar to what we have today with software components in the cloud and on premise. Such arrangements will be supported by a new concept that the IIC terms an Industrial Internet Monetization Model (I^2M^2) platform. Complete industrial systems are a collection of components based on a specific setup. Therefore, such business models and payment models can be expanded to whole systems including the system integration work. Such business models and payment organizations include: • Leasing/subscription: a component is paid in frequent intervals, for example monthly, during the time of the usage. • Feature on demand: a component part is not paid until it is required for the first time. • Pay per use: the component or specific features are only paid for if they are used. • Revenue and profit sharing: The provider of the component is paid depending on specific business value the component provides to the user. • Freeware: core features are free; only advanced features are sold. • Trialware: specific features can be tried for a limited time for free before the user is charged.
Key usage scenarios: • Reducing upfront payments for risky industrial systems with the opportunity for future “share of success” of the component deliverer. • Setup of industrial systems that cannot be realized today due to high investment risk and lack of funds. • Repeated revenue of component deliverers during the full lifetime of the component.

DX Technology: Technical Platforms for New Business Models and Payment Models
• Active lifetime business relationship between component manufacturer and user.
Relevant IIC publications: • I²M²—the Future of Industrial System Monetization, Journal of Innovation March 2018[1]
Opportunities for the IIC: • Refining specific business processes around IIoT systems. • Presenting and discussing new business and payment models to component manufacturers, system integrators, payment processors and end users who operate industrial systems. • Preparing work for standardizing the automatic installation, processing and management of new business and payment models

Table 2-15: Technical Platforms for New Business and Payment Models

3 Digital Transformation and Trustworthiness

The word "trustworthy" is an adjective that describes the quality of an object: a person, an organization, a system and so on. We cover trustworthiness here as it applies to IoT-enabled systems in the context of digital transformation.

3.1 What is Trustworthiness in IoT?

IoT technologies are a foundation stone of digital transformation. IoT technologies must be trustworthy so they can enable a DX journey using the techniques and approaches below. Trustworthiness of IoT-enabled systems is the degree of confidence that an IoT system will perform as expected with characteristics including safety, security, privacy, reliability and resilience in the face of environmental disturbances, human errors, system faults and attacks. Individuals and organizations are increasingly aware of how data is used and protected, leading to increased regulation and social standards around trustworthiness.

[1] *https://www.iiconsortium.org/news/joi-articles/2018-March_IIoTFuture_Industrial_System_Monetization_Wibu.pdf*

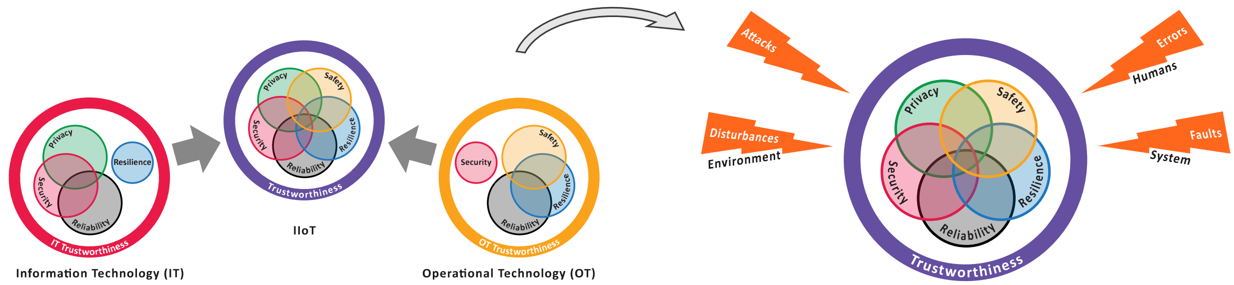

Figure 3-1: Convergence of IT-OT and IoT Trustworthiness–source IIC

3.2 IoT Trustworthiness Requirements

An IoT system is trustworthy if it meets the minimum requirements for each of the five characteristics as defined above. These minimum requirements are in some cases mandated by laws, regulations, standards, and industry-accepted best-practices. These requirements are applicable throughout the lifecycle of an IoT system.

Privacy and safety examples of regulatory constraints include EU GDPR privacy laws or OSHA workplace safety standards. Reliability and resilience are often driven less by laws than by competitive forces, though some are heavily regulated, such as aerospace or healthcare. Most organizations should strive to remain at, or above, the minimum requirements for each of the five factors to ensure that they comply with regional requirements and industry best practices.

Beyond this minimum level, enterprises can establish higher targets for trustworthiness based on corporate vision, roadmap, and market positioning.

Figure 3-2 below depicts the trustworthiness states of an example IoT-system: current (red), minimum (blue) and target (green). In this spider diagram, the current state of safety for that example system appears to meet the minimum requirements while the other characteristics of trustworthiness, namely security, privacy, reliability and resilience fall short.

Current State
- Actual state as it exists now
- May change over time

Minimum State (external drivers)
- Min non-negotiable and mandated level
- Laws, regulations, standards, best practices, etc.
- Jurisdictional variations

- *Laws, Regulations*
- *De-Jure Standards*
- *Best Practices*
- *Example: OSHA 29 CFR 1910, IEC 61508, EU GDPR, CCPA*

Target State (internal drivers)
- Objective level to achieve
- Alignment with corporate vision, ROI, risk, etc.

- *Corporate vision & mandate*
- *Competitive positioning*
- *Strategy for risk reductions*
- *Technical Roadmap*

Figure 3-2: Different Trustworthiness States–source IIC

In IoT trustworthiness, the consequences of "acting badly" (red line falling short of the blue line) can include the loss of human life, negative long-term impact on the environment or the interruption of critical infrastructure, and the unintended disclosure of sensitive data, destruction of equipment, economic loss and reputational damage.

3.3 Impact of Trustworthiness on Digital Transformation

These negative consequences can put a digital transformation journey at risk. A lack of trustworthiness may mean that windows of opportunities in the market may be missed forever, placing the organization at a disadvantage vis-à-vis its competitors.

Even with the benefits associated with achieving baseline levels of trustworthiness, too much trustworthiness is not always a net-positive for an organization, as listed below:

Trustworthiness Characteristics	Possible consequences of excessive emphasis
Security	Increased costs, loss of agility and reduced usability.
Safety	Reduced solution flexibility, more complex processes and reduced productivity.
Reliability	Excessive capital and maintenance costs; reduced usability.
Resilience	Excessive capital and maintenance costs, reduced flexibility and functionality.
Privacy	Unnecessarily cumbersome processes.

Therefore, there are often compromises made between the risk of underinvesting in trustworthiness efforts and the consequences of overinvesting in it. Putting trustworthiness in the context of a business case often highlights trade-offs, as illustrated in figure 3-3 below.

This example relates to a small batch assembly line for electronic boards. The nature of this process is such that the assembly machines may need to be recalibrated and reconfigured between different batches. Slowing down the assembly line may reduce the risks personnel injury and levels of equipment wear and tear, and it may reduce productivity and profits[1].

[1] Refer to the Managing and Assessing Trustworthiness for IIoT in Practice whitepaper *https://www.iiconsortium.org/pdf/Managing_and_Assessing_Trustworthiness_for_IIoT_in_Practice_Whitepaper_2019_07_29.pdf*

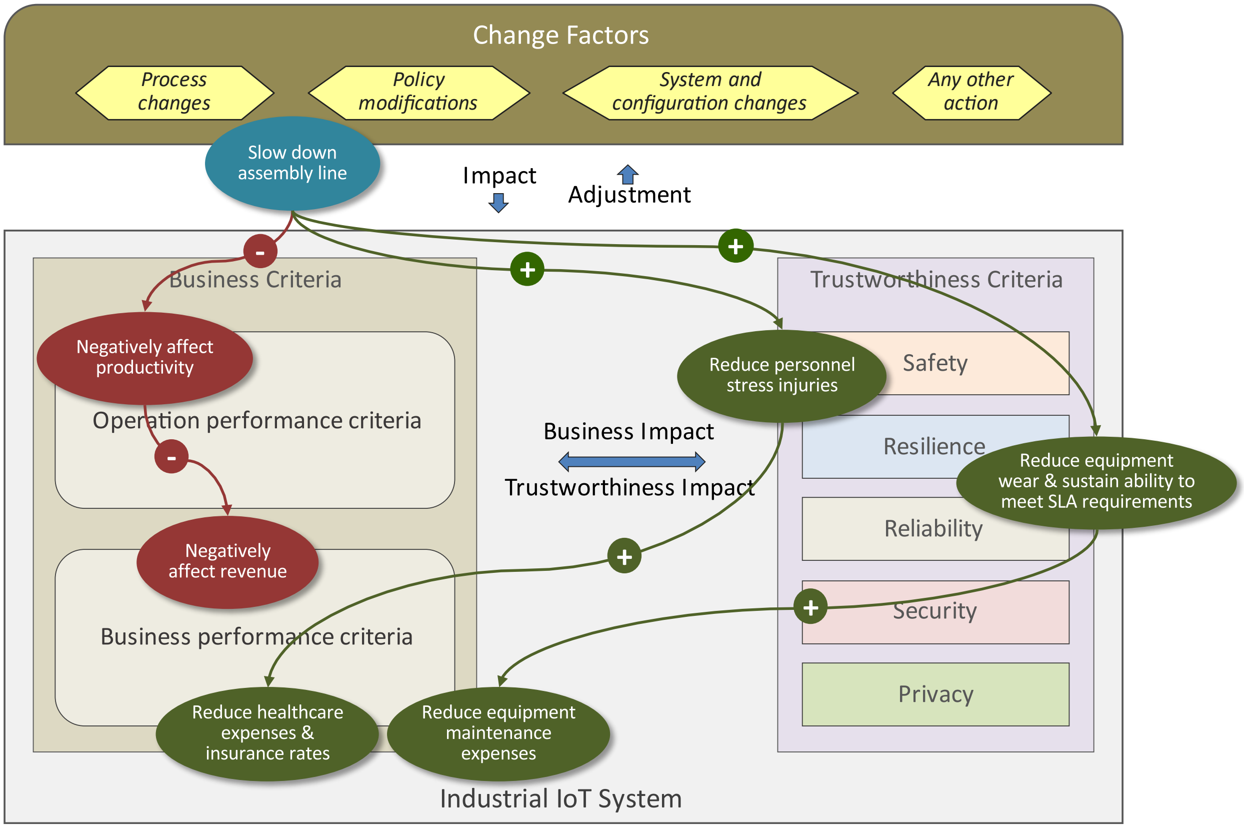

Figure 3-3: Example of Trustworthiness Analysis–source IIC

Of course, there can be financial benefits associated with investing more in trustworthiness:

- reduced number of compensatory payments to customers for failures,
- reduced legal and regulatory risk and of fines for non-compliance with regulations,
- reduced reputational risk,
- increased sales and revenue due to stronger brand image,
- reduced costs of business insurance,
- reduced costs of funding for non-determined risks and
- increased shareholder-value.

The main challenge and goal are to identify an 'optimum' balance of trustworthiness as defined by an organization's current state, minimum requirements, and target state. This optimization approach also applies to the organization's entire digital transformation effort and to the overall trustworthiness strategy and associated level of investment.[1]

[1] Refer to the Managing and Assessing Trustworthiness for IIoT in Practice whitepaper *https://www.iiconsortium.org/pdf/Managing_and_Assessing_Trustworthiness_for_IIoT_in_Practice_Whitepaper_2019_07_29.pdf*

4 CONTEXT FOR THE DX JOURNEY

Digital transformation is a strategy that requires a "by design" approach and way of thinking (rather than "by accident"). We provide context for the role of innovation in DX and the organizational changes that such transformation requires.

4.1 ROLE OF INNOVATION IN DIGITAL TRANSFORMATION

An industrial organization needs to set up innovation processes that are different from existing processes in several ways, including:

- This process includes exploring feasibility of applying new technologies, integrating IT and OT and the creation and operation of solutions that combine OT and IT.
- The process is a "fast" process based on building a "minimum viable product", inheriting the traditions of lean start-up, design thinking and BizDevOps.[1]
- An "open" process of innovation dealing with the complexity of integrating OT and IT, enabled by cooperation among different divisions and different firms (including IT and OT organizations). With extensive use of IT, leveraging connected things and people, the process should enable open interaction with partners, customers and suppliers in IT and OT domains. In the "open" process, the IT & OT organizations learn each other's domain knowledge and understand each other's constraints, problems and discover collaboration issues for solving the problems.
- Optimized processes for creating solutions for customers, delivering better customer experiences and/or outcomes, leveraging connected things and people including customers, which can be achieved with a customer centric mind set.

> **Important:** The innovation processes are continually vulnerable to resistance from both OT and IT organizations and are likely to conflict with incumbent processes and organizational structures and other aspects of existing management systems.

The process change is made possible by creation and diffusion of innovation tools (for example, GE's FastWorks[2]) for 'fast, open and efficient' innovation processes integrating IT and OT. The diffusion of tools can be facilitated by removal of conflicts of new innovation processes with incumbent management systems including incumbent processes, organizational structures, employee evaluation system, cultures and innovation funding system through changes of the management system.

[1] BizDevOps is a collaborative culture which enables a new model of operating (business, operations and technology together) to produce superior products and services through an automated pipeline (PwC) *https://www.digitalpulse.pwc.com.au/bizdevops-competitive-advantage/*

[2] *https://www.gartner.com/smarterwithgartner/why-big-companies-need-lean-startup-techniques/*

The changes lead to gradual progress in digital transformation. Digital transformation can thus be achieved by accumulating results from ongoing innovation initiatives exploring new value propositions. Better customer experiences and outcomes gradually emerge from the integration of IT and OT, with a customer-centric mind set to leverage connected things and people.

4.2 The Digital Transformation Program

Digital transformation is not a project. It is strategy, and a journey, led by a vision, powered by a committed program, which in turn is a set of related activities with long-term aim.

The DX program must have a well-defined objective, charter, mission, and governance structure. The program must also be guided by a cross-functional team with a clear leader and a corporate sponsor, with active participation from several cross-functional stakeholders (figure 4-1) who must work together in a structured way to achieve the better outcomes.

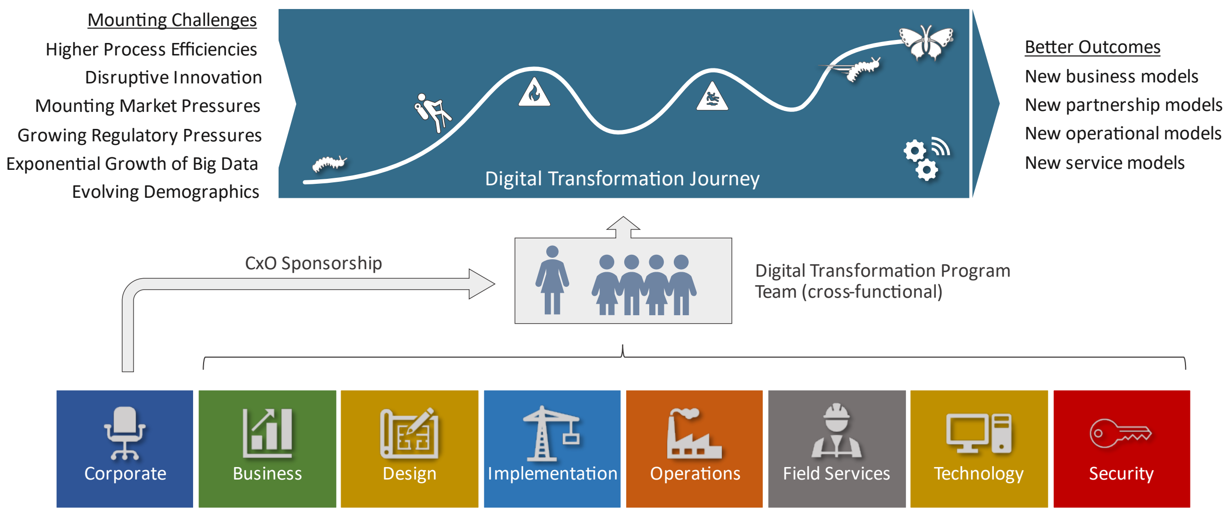

Figure 4-1: Cross-functional Digital Transformation Program Team–source IGnPower

The *DX program corporate sponsor* directs the DX program team leadership to achieve the DX objectives and empowers it with authority, resources, and funding. Depending on the organization, this individual may have a CxO title, such as CEO, CDO (Digital), CMO, COO, CIO, etc.

The *DX program team leader* leads the DX program and reports (may be dotted line) to the corporate sponsor. The type of organization, industry and scope of digital transformation affects from which group the leader comes. The team leader must maintain a communication strategy with the corporate sponsor and the various stakeholders of the DX program:

- progress of the DX program and projects within it,
- coordination and alignment of activities by different stakeholders,
- value being delivered by the DX program to individual stakeholders,
- challenges facing the program and its projects and
- planning of program and project activities.

The *DX program team* directs and supervises the DX program. It is tasked, empowered, and made accountable for delivering the concrete "output" and tangible "business benefits" of the program. The team brings together multiple stakeholders that come from siloed communities with their own budgets, reporting structure, techniques, assessment practices, standards, and regulations), based on considerations such as:

- type of organization and industry,
- drivers and urgency levels behind the transformation,
- competitive landscape,
- nature of the disruptive technologies enabling the transformation and
- scope of expected better outcomes.

One of the main responsibilities of this team is to market the value of DX strategy to the different DX stakeholder groups in the organization effectively.

Moreover, the DX program may involve several IIoT projects. Each project may have its own set of stakeholders and expectations. It is the responsibility of the DX program team to coordinate with the various IIoT project teams to ensure that the projects remain aligned with the DX strategy and continue to deliver the benefits to the organization intended by that strategy.

Note: Some organizations have an established Chief Digital Officer role (CDO). This individual may be the corporate sponsor of the DX program or the leader of that team.

4.3 DX Programs and IIoT Projects

The organization's journey of digital transformation in industry may involve the implementation of multiple IIoT technology projects that can enable and, in some cases, drive the transformation sought. These projects must support, within their requirements and the definition of their deliverables, the ability to address the mounting challenges and achieve the desired better outcomes (figure 4-2).

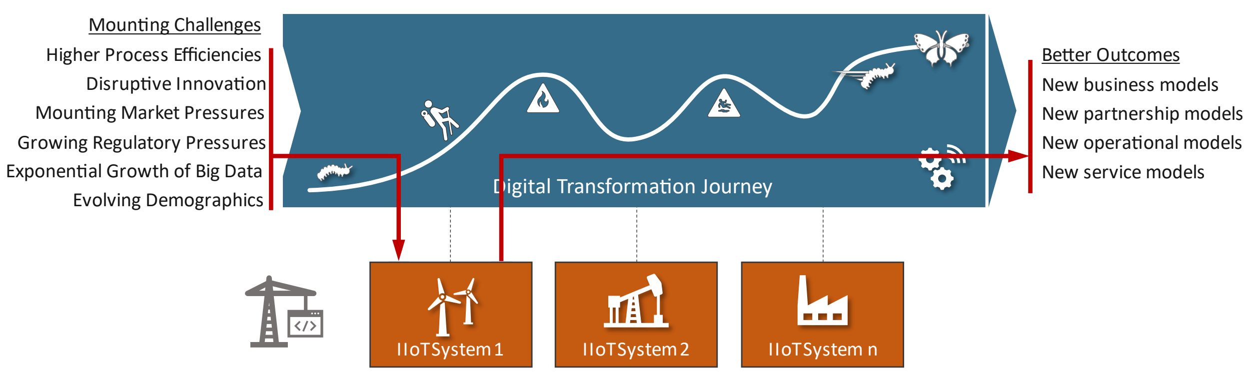

Figure 4-2: Digital Transformation Programs and IIoT Projects–source IIC

For IIoT projects that are already under way when the digital transformation strategy is defined, the scope of these projects must be reviewed to analyze, assess and perhaps adjust their scope to maximize their impact and contribution to the digital transformation strategy.

5 First Steps for Adoption

Digital transformation is a type of disruption. It will unlock new possibilities in business models, value propositions and operational efficiency. Competitive dynamics will ensure that entire industries must transform to become a market leader or keep pace with market leaders, or face loss of market share. As ever, this kind of disruption is not risk-free.

The key is to minimize the attendant risks. Our recommended approach is that industry users follow the 'First Steps for Adoption' framework, shown in figure 5-1, and discussed below.

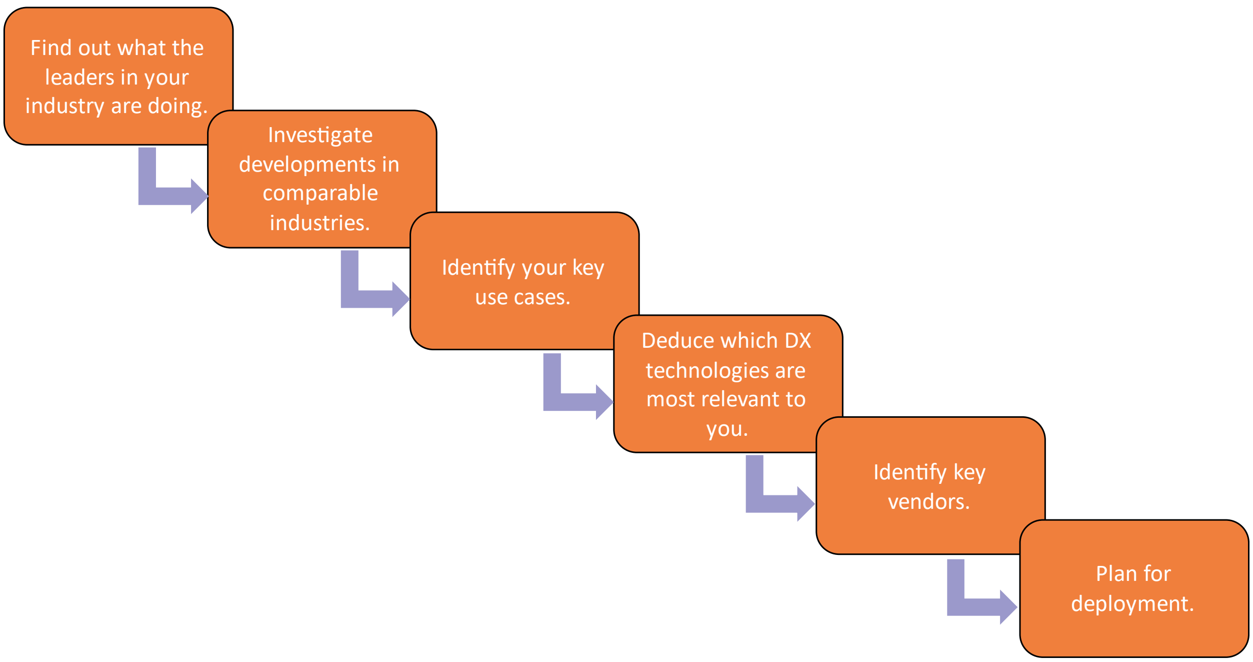

Figure 5-1: First Steps for Adoption Framework–source Transforma Insights

5.1 Find out what the leaders in your industry are doing

The first question is to determine what your competitors are doing, since competitor actions are likely to be the source of the most immediate threats and risks.

Unless you are the established technology market leader in your industry, then the most effective strategy is usually that of a 'fast follower'. The advantages of a fast follower strategy are a combination of reduced risk (only matching competitor initiatives that seem likely to be effective) and speed (taking action quickly, before any initiatives that competitors have undertaken have been able to have a material market share impact).

5.2 INVESTIGATE RELEVANT DEVELOPMENTS IN COMPARABLE INDUSTRIES

Next, research digital transformation initiatives in comparable industries, and assess the potential impact of these for your own situation. While many industries might at first appear to be fundamentally different, there may be digital transformation approaches and solutions being pioneered in one that are potentially relevant to another. Examples include:

- solutions to support the management of construction machinery on building sites, providing insight into the best approach for managing the availability of medical devices in medical environments,
- facial recognition and people-tracking solutions used in the public sector can be adapted for use in arts & entertainment industries, or in retail parks and
- the advent of pay-as-you-drive insurance solutions supporting shared-car propositions, providing lessons learned for warranty management when offering goods-as-a-service.

Another approach is to identify projects in other industries that have in some way faced 'similar' challenges to those at hand. For instance, if you are planning to roll out multiple-millions of devices into a highly regulated market, then analysis of others who have already overcome these challenges might yield useful lessons.

The range of possibilities for cross-pollination of digital transformation ideas between industries is endless. This kind of analysis can provide a ready-made list of best practices drawn from across all industries, and can provide insight into the likely future development of any given industry.

5.3 IDENTIFY YOUR KEY USE CASES

Benchmarking research has focused on analyzing real-world digital transformation projects, but these can be aggregated to a generic 'use case' level. For instance, multiple competitors might be working on fleet management solutions. But what is most relevant to you in planning your own solution is the generic capabilities and benefits that fleet management solutions can unlock rather than the detail of any specific case study.

The approach is for the end-user to develop a vision of their own fleet management solution, informed by the lessons learned and results achieved from the identified case studies.

5.4 DEDUCE WHICH DIGITAL TRANSFORMATION TECHNOLOGIES ARE MOST RELEVANT TO YOU

The next step is to identify which are the critical enabling technologies for the identified use cases. Continuing with the fleet management use case, key technologies would be IIoT, edge computing and AI. An industry user must develop some familiarity with these underlying technologies, as it will make future interaction with the vendor community more efficient and effective.

5.5 Identify key vendors

Many technology vendors have broad experience of digital transformation in a range of verticals. But the key vendors for an individual industry user will have deep knowledge of the technologies most relevant to the user in question, and extensive experience of that users' industry. Ideally, key vendors will also have experience across multiple geographies, so that 'lessons learned' from one geography can be more readily ported to the users' home geographies.

Many large vendors will offer extensive educational documentation, together with independent analyst and consulting publications identifying opportunities, sharing best practices and lessons learned from case studies. Many leading vendors will also offer 'experience centers' where new technologies can be tried in an environment that is supported by the vendor, and with easy access to vendor expertise.

It is critical for any end user considering the deployment of DX solutions to identify their own key vendors, and to build strong relationships with them.

5.6 Plan for deployment

The IIC has a range of resources that help planning for next steps, including framework publications (for example the Business Strategy Innovation Framework[1]), technical publications (for example the Introduction to Edge Computing in IIoT white paper), and web tools available via the Resource Hub.[2]

Additionally, the Accelerator Program has testbeds, test drives and challenges that are technology-, solution- and application-focused respectively.

1 *https://www.iiconsortium.org/BSIF.htm*

2 *https://hub.iiconsortium.org/homepage*

6 ACKNOWLEDGEMENTS AND LEGAL

This document is a work product of the Industrial Internet Consortium Digital Transformation Working Group, co-chaired by Jim Morrish (Transforma Insights), Dirk Slama (Bosch) and Bassam Zarkout (IGnPower).

Editors:

- Jim Morrish (Transforma Insights)
- Bassam Zarkout (IGnPower)

Authors (in alphabetic order):

- Marcellus Buchheit (Wibu-Systems)
- Alex Ferraro (PwC)
- Chaisung Lim (Korea Industry 4.0 Association)
- Shi-Wan Lin (Yo-i Information Technologies, Ltd.)
- Jim Morrish (Transforma Insights)
- Bassam Zarkout (IGnPower)

Technical Editor: Stephen Mellor (IIC staff) oversaw the process of organizing the contributions of the above Authors and Contributors into an integrated document.