



Industrial IoT Artificial Intelligence Framework

2022-02-22

Authors

*Wael William Diab, Alex Ferraro, Brad Klenz, Shi-Wan Lin,
Edy Liongosari, Wadih Elie Tannous, Bassam Zarkout.*

CONTENTS

1	Industrial Artificial Intelligence.....	6
1.1	Industrial Internet of Things.....	6
1.2	Industrial Artificial Intelligence	6
1.3	Architecture Viewpoints	7
2	Business Viewpoint.....	8
2.1	Uncover Valuable Insights From Data Intensive Environments	9
2.2	Enable Digital Transformation.....	9
2.3	Agent for Future-Proofing the Organization.....	11
2.4	AI Adoption Readiness.....	11
3	Usage Viewpoint.....	12
3.1	Industrial AI Market.....	12
3.2	Usage Considerations	13
3.3	Trustworthiness	15
3.3.1	Security	16
3.3.2	Privacy.....	19
3.3.3	Confidentiality.....	20
3.3.4	Explainability.....	21
3.3.5	Controllability	21
3.4	Ethical and Societal Concerns.....	22
3.4.1	Ethics.....	22
3.4.2	Bias.....	23
3.4.3	Safety	24
3.5	Impact on Labor Force	25
3.6	Regional and Industry-Specific Considerations.....	27
3.7	AI as a Force for Good.....	27
4	Functional Viewpoint	28
4.1	Architecture Objectives and Constraints.....	28
4.2	Data Concerns	29
4.3	Learning Techniques.....	30
4.4	General Industrial AI Functional Architecture	32
4.5	System of Systems Issues.....	34
4.6	Application Horizon of Industrial AI.....	35
5	Implementation Viewpoint	36
5.1	Implementation Guidance	36
5.2	Implementation Considerations.....	37
5.2.1	Scope.....	37
5.2.2	Response Time	37
5.2.3	Reliability	38
5.2.4	Bandwidth and Latency	38
5.2.5	Capacity.....	39
5.2.6	Security	39
5.2.7	Data Properties	39

Industrial IoT Artificial Intelligence Framework

5.2.8	Temporal Data Correlation	40
5.2.9	Interoperability	40
5.2.10	Running Systems In Parallel.....	40
5.2.11	Dealing With Technical Debt.....	41
5.2.12	Portability and Reusability of AI Systems	41
6	The Future of the Industrial AI.....	42
6.1	Far-Reaching Benefits of AI Despite the Risks	42
6.2	Convergence with Other Transformative Technologies	42
6.3	Standards Ecosystem	44
6.3.1	Enabling intelligent insights	45
6.3.2	Ecosystem approach	46
6.3.3	Program of work and role in enabling DX across industries.....	46
6.3.4	Summary	48
6.4	Final Thoughts and Takeaways.....	48
Annex A	Artificial Intelligence Background	50
A.1	Brief History of AI	50
A.2	Why Now?	51
A.2.1	Cheap and Powerful Compute Infrastructure	51
A.2.2	Availability of Large Amounts of Data	52
A.2.3	Improvements in Algorithms	52
Annex B	Exemplary Use Cases of AI in Industry	52
B.1	Manufacturing.....	53
B.2	Healthcare.....	55
B.3	Buildings	56
B.4	Transportation and Logistics	57
B.5	Detecting IIoT System Threats Using AI	57
Annex C	IIC References	58
Annex D	Authors & Legal Notice.....	59

FIGURES

Figure 1-1. Industrial Internet Viewpoints. Source: IIC IIRA.	7
Figure 2-1. Industrial AI Framework Business Viewpoint. Source: IIC.	8
Figure 2-2. Digital Transformation Journey. Source: IIC.	10
Figure 3-1. Industrial AI Framework Usage Viewpoint and Its Stakeholders. Source: IIC.	12
Figure 3-2. Trustworthiness of IIoT Systems. Source: IIC.....	15
Figure 3-3. Security Framework Functional Building Blocks. Source: IIC IISF.	17
Figure 3-4. Skill shift: Automation and the Future of the Workforce. Source: McKinsey.	26
Figure 4-1. Industrial AI Framework Functional Viewpoint and Its Stakeholders. Source: IIC.	28

Industrial IoT Artificial Intelligence Framework

Figure 4-2. AI/Machine Learning Model Process.....	29
Figure 4-3. Data Processing for AI Modeling.	30
Figure 4-4. Industrial AI System.	31
Figure 4-5. Industrial AI in Industrial Operation Environment.	32
Figure 4-6. Industrial AI High-Level Functional Components.	33
Figure 4-7. Example of a System of Systems in the EV Charging Space. Source: Artemis.	34
Figure 5-1. Industrial AI Framework Functional Viewpoint and Its Stakeholders. Source: IIC.	36
Figure 6-1. Trustworthiness of IIoT Systems. Source: ISO /IEC JTC 1/SC42.	46

TABLES

Table 3-1. Key Roles of AI in Industrial Applications.....	14
Table 3-2. Securing Industrial AI Across the IIoT Security Function Building Blocks.	18
Table 3-3. Core Principles of the AI Ethics Framework. Source: Department of Industry, Australia.	23

Industrial Artificial Intelligence (AI) is the use of AI in applications in industry¹ and a major contributor to value creation in the fourth industrial revolution. AI is being embedded in a wide range of applications, helping organizations achieve significant benefits and empowering them to transform how they deliver value to the market.

This document provides guidance and assistance in the development, training, documentation, communication, integration, deployment and operation of AI-enabled industrial IoT systems. It is aimed at decision makers from IT and operational technology (OT), business and technical from multiple disciplines, including business decision-makers, product managers, system engineers, use case designers, system architects, component architects, developers, integrators and system operators.

The document is structured around the architecture viewpoints as framed in IIC's *Industrial Internet Reference Architecture*, namely business, usage, functional and implementation viewpoints. The document discusses the business, commercial and value creation considerations that drive the adoption of AI. It also elaborates on the concerns that arise from the usage of AI, the use cases in industry, and the ethical, privacy, bias, safety, labor impact and societal concerns related to them. On the technical side, the document describes the architectural, functional and data considerations related to AI, and discusses various implementation considerations, such as performance, reliability, data properties and security.

The adoption of AI is expected to accelerate in the industry. AI technology will continue to evolve, given the fast-increasing compute power, wider availability of data that can be used for training and the ever-growing sophistication of algorithms. Current IT standards and best practices must evolve to address the unique characteristics of AI itself and specific considerations related to safety, reliability and resilience of IIoT systems. In addition, the growing maturity of organizations about AI will help them appreciate that its benefits far outweigh its risks. The AI standards ecosystem will also continue to evolve, for example the ongoing standards work by ISO/IEC JTC 1/SC42 that provides guidance to JTC 1, IEC and ISO committees developing AI standards.

Based on these trends, there should be little doubt that AI will continue to push the state-of-the-art of what is technologically and functionally possible, and thus what is expected to be the reasonable thing to do will equally evolve. Attitudes towards the technology and business expectations about its use will also continue to evolve.

In the future, we can expect the use of AI technologies to become the norm rather than the exception, and given the societal benefits of this technology, “not using AI” may eventually become the irresponsible thing to do.

¹ Smart manufacturing, robotics, predictive maintenance, health diagnostics, and autonomous vehicles.

1 INDUSTRIAL ARTIFICIAL INTELLIGENCE

This section introduces the Industrial Internet of Things (IIoT) and the application of Artificial Intelligence (AI) in IIoT ecosystems (Industrial AI). It focuses on the considerations that must be addressed during the AI's full lifecycle within an IIoT system, from design to implementation and operation.

1.1 INDUSTRIAL INTERNET OF THINGS

The Industrial Internet of Things integrates the industrial assets and machines—the things—with enterprise information systems, business processes and people who operate or use them.

With these connections to the industrial assets and machines, modern technologies enable the application of AI to machine and operational process data to gain insights into the operations, optimize them intelligently to boost productivity, increase quality, reduce energy and material consumption, increase flexibility and ultimately create new business value. All this must be done while maintaining commitments to safety, reliability, resilience, security and data privacy as the trustworthiness of the systems and conservation of the environment as social values.

IIoT is a natural extension of the industrial and internet revolutions. IIoT is a major force driving economic growth, now and for the coming decades, at a greater pace than prior revolutions. As outlined by the World Economic Forum,² “The first industrial revolution used water and steam power to mechanize production. The second used electric power to create mass production. The third used electronics and information technology to automate production. Now, a fourth industrial revolution is building on what has preceded it, blurring the lines between the physical, digital and biological spheres.”

To accelerate this digital revolution the Industry IoT Consortium (IIC) is advancing the technology of IIoT across a diverse set of application domains.

1.2 INDUSTRIAL ARTIFICIAL INTELLIGENCE

Industrial artificial intelligence is the application of AI to IoT applications in industry, in areas like smart manufacturing, robotics, predictive maintenance, diagnosis of infectious disease with machine learning and autonomous vehicles.

The use of AI is pervasive in the enterprise, helping organizations achieve significant benefits in terms of better insight, faster decisions and more effective operations. In particular, AI plays a key role in driving the IT/OT convergence with a growing range of practical applications in industry, for example automating routine labor tasks, driving autonomous vehicles,

² World Economic Forum (2016): *The Fourth Industrial Revolution: What it Means, How to Respond*. <https://bit.ly/3CRmjzz>.

understanding speech and performing medical diagnostics. Industrial AI is a major contributor to value creation in the fourth industrial revolution.

1.3 ARCHITECTURE VIEWPOINTS

This Industrial AI Framework uses the architecture viewpoints of the IIoT, viewpoints for short, as defined in the IIC Industrial Internet Reference Architecture³ (IIRA):

- Business Viewpoint,
- Usage Viewpoint,
- Functional Viewpoint and
- Implementation Viewpoint.

This reference architecture document leverages the ISO/IEC/IEEE 42010:2011⁴ methodology to identify these viewpoints. We highlight four important terms from this standard as they are used throughout this document.

Stakeholders are individuals, teams, or organizations that have an interest in a system. *System concerns* are interests in a system relevant to one or more of its stakeholders. *Architecture views* are work products expressing the architecture of a system from the perspective of specific system concerns. *Architecture viewpoints* are work products that establish the conventions for the construction, interpretation and use of architecture views to frame specific concerns

The architecture viewpoints identify relevant stakeholders and their concerns and articulates how these concerns are addressed. A stakeholder may have more than one type of concern, for example an executive may have business concerns as well as concerns about implementation; a system architect may have usage concerns as well as functional and implementation concerns.

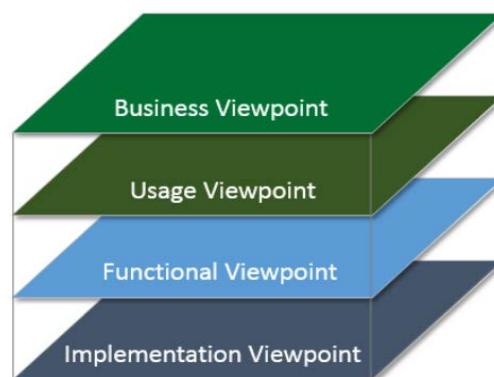


Figure 1-1. Industrial Internet Viewpoints. Source: IIC IIRA.

The viewpoints provide different perspectives of the complex IIoT system and taken together (see Figure 1-1) express the system's architecture.

³ IIC: *Industrial Internet Reference Architecture*. Refer to Annex C for details.

⁴ <https://www.iso.org/standard/50508.html>

The *business viewpoint* attends to the concerns of the identification of stakeholders and their business vision, values and objectives in establishing an IIoT system in its business and regulatory context. It further identifies how the IIoT system achieves the stated objectives through its mapping to fundamental system capabilities.

The *usage viewpoint* addresses the concerns of expected system usage, typically represented as sequences of activities involving human or logical (e.g. system or system components) users that deliver its intended functionality, ultimately achieving its fundamental system capabilities.

The *functional viewpoint* focuses on the functional components in an IIoT system, their structure and interrelation, the interfaces and interactions between them, and the relation and interactions of the system with external elements in the environment, to support the usages and activities of the overall system.

The *implementation viewpoint* deals with the technologies needed to implement functional components (functional viewpoint), their communication schemes and their lifecycle procedures. These elements are coordinated by activities (usage viewpoint) and supportive of the system capabilities (business viewpoint).

For AI technology, the architecture viewpoints can help current and aspiring providers and operators of AI-enabled IIoT systems to identify and gauge the value that AI technology can bring to the system's design and operation. The viewpoints facilitate a systematic way to identify industrial AI system concerns and their stakeholders and bring similar or related concerns together so they can be analyzed and addressed effectively. The deliberation of the concerns is often performed within each of the viewpoints to which they belong, but they should not be resolved in isolation to those in other viewpoints.

2 BUSINESS VIEWPOINT

The business viewpoint attends to the concerns of stakeholders including business decision makers, for example executive officers, board of directors, general managers, as well as technical managers and plant managers. The viewpoint encompasses their business vision, values and objectives in establishing an AI-enabled IIoT system in its business and regulatory contexts.

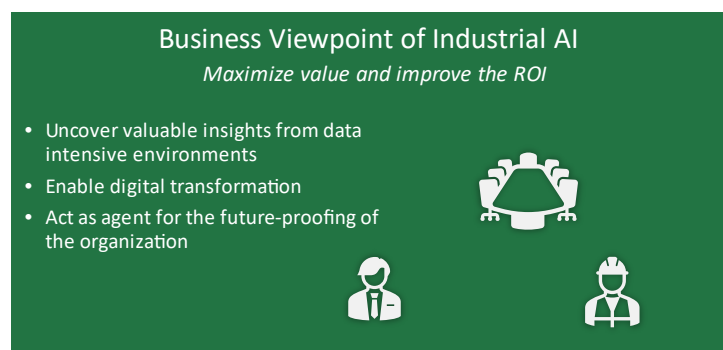


Figure 2-1. Industrial AI Framework Business Viewpoint. Source: IIC.

As Figure 2-1 shows, the primary consideration of this viewpoint is to maximize value to the organization and its ecosystem through a direct improvement of the ROI. For example, AI can more effectively provide insights such as increasing production throughput, avoiding or reducing operating costs, delivering higher margins, enabling new capabilities, minimizing mistakes, reducing inventory, improving safety, making better and faster decisions and improving the quality of products.

The application of AI can also maximize value indirectly as a result of improving societal aspects. For example, AI can increase the accuracy of disease diagnosis, help experts predict natural disasters better, improve education through one-on-one tutoring of students, promote a gradual evolution in the job field and reduce on-the-job hazards by enabling automated systems and robots to do hazardous tasks. These indirect (and not so indirect) benefits can also lead to improvements of the organization's ROI.

2.1 UNCOVER VALUABLE INSIGHTS FROM DATA INTENSIVE ENVIRONMENTS

IIoT systems with connected devices, people, and environments generate significant amounts of data with complex relationships across the organization's silos and ecosystems.

This overwhelming amount of data exhibits the typical characteristics of big data such as volume, variety, velocity, veracity and value (or lack thereof). "Value" can be elusive, but the organization can use AI to analyze and uncover valuable insight from this data. This can help the organization identify ways to improve the ROI, make effective decisions and uncover hidden risks that the organization may be facing: financial, operational, governance-related, etc.

AI enables value capture across an increasingly diverse array of use cases and industries. One research briefing estimates that AI applications have the potential to create between \$3.5 trillion and \$5.8 trillion in value annually across nine business functions in 19 industries.⁵

Another study estimates that by 2030, AI will provide a 26% boost in GDP, equivalent to a \$15.7 trillion⁶ contribution to the economy. The most important value driver for AI is not the technology itself but "the proximity of where it is applied to profits."⁷

2.2 ENABLE DIGITAL TRANSFORMATION

The application of AI technology can help transform the enterprise into a smart digital enterprise and enable the creation of new and transformative types of businesses. AI can also act as a

⁵ McKinsey: *Notes from the AI Frontier: Applications and value of AI deep learning*. <https://mck.co/3k4qIMe>.

⁶ PwC: *Sizing the prize, PwC's Global AI Study, Exploiting the AI Revolution*. <https://pwc.to/384ugU5>.

⁷ Forbes: *Past the AI Hype: When is AI Actually Profitable*. <https://bit.ly/3g9Lu6V>.

catalyst for digital transformation (DX) initiatives⁸ that can generate more value for the organization than product design IP.⁹

Digital transformation is a journey (see Figure 2-2) from the “mounting challenges” facing the organization to the “better and transformational outcomes” that can address these challenges. The journey is underpinned by business, technology and trustworthiness factors.

Achieving success in the DX journey requires the active engagement of the stakeholders who will invariably bring different perspectives and diverging expectations about what DX means for them: strategy, program, process, project(s) or technologies.¹⁰

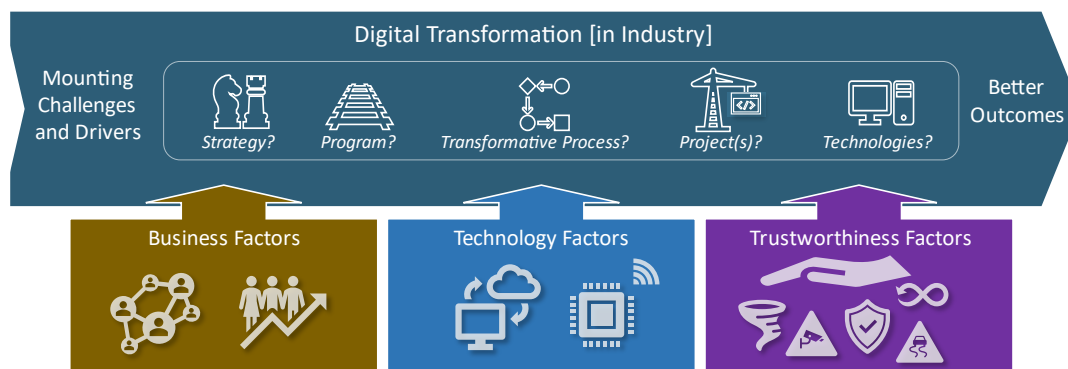


Figure 2-2. Digital Transformation Journey. Source: IIC.

AI plays a significant role in disrupting the organization and empowering its digital transformation journey. While some applications of AI are niche and selective, most are disruptive and transformative in nature.

Back in 2019, IDC predicted that by 2021 75% of DX initiatives will leverage AI services. This prediction has held true. AI is allowing organizations to become more innovative, more flexible, more efficient and more adaptive. In an industrial context, it is enabling machines to ensure that machines operate properly and optimally, measuring and optimizing productivity of processes and providing predictive maintenance recommendations.

AI-based IIoT systems are also opening up opportunities to commercial and public entities to re-assess, optimize and re-deploy their workforce for the emerging digital workplace.

⁸ IIC (September 2020): *Digital Transformation in Industry white paper*.

⁹ *Digital Transformation, Survive and Thrive in an Era of Mass Extinction, Chapter 3*. Thomas Siebel. <https://amzn.to/2W25j9d>.

¹⁰ IIC Journal of Innovation (November 2021): *The Digital Transformation Journey in the Enterprise and its Leadership*.

2.3 AGENT FOR FUTURE-PROOFING THE ORGANIZATION

An AI-powered digital enterprise is a smart digital enterprise that has the capacity to look forward and use AI as an early warning system about issues that have not been thought about such as business threats and missed business opportunities. This is equivalent to finding out about what “you do not know what you do not know”. This can take the organization to a different level.

The capacity of AI to act as an agent for such a “future proofing” role is especially valuable for organizations where converging IT and OT systems require that functions that execute in IIoT systems be integrated with functions that execute in business systems. This involves a complex merge of key system characteristics, best practices and organizational cultures. AI technology is uniquely suited to span such integrated IT/OT environments and uncover threats and opportunities that are not possible for humans to discern.

In addition to its profound impact on organizations, AI may ultimately redefine the strategic value of IT for organizations, raising the stakes for the need for AI governance.

2.4 AI ADOPTION READINESS

Most AI-focused publications focus on the design and development considerations of the AI models themselves. This section focuses on the readiness and maturity requirements¹¹ needed to make AI models work for enterprises (industrial or otherwise), how to define requirements for AI applications, how to improve AI models continuously in terms of application and domain-specific correctness, accuracy, fairness for those applications in the social settings and how to customize general-purpose models to specific use cases.

In general, to achieve maturity in AI environments, there should be an emphasis on:

- automation: offering new possibilities for both clients and stakeholders,
- information sharing: offering predictions and insights to decision-makers and planners,
- discovery: offering a baseline for more effectiveness and efficiency and
- transformation: offering an intelligence driven enterprise.

Gartner further breaks down AI maturity into five levels:¹²

- Level 1, Awareness: Early AI interest with risk of overhyping,
- Level 2, Active: AI experimentation, mostly in data science context,
- Level 3, Operational: AI in production, creating value,
- Level 4, Systemic: AI is pervasively used for digital process and chain transformation and
- Level 5, Transformational: AI is part of business DNA.

Gartner suggests that organizations aspiring to use AI effectively should aim to be at maturity level 3 or higher (machine learning in its functions, having ML engineers to maintain models and

¹¹ IBM: Characterizing Machine Learning Process: A Maturity Framework. <https://bit.ly/3k1zbun>.

¹² Gartner: *AI Maturity Model G00466009 (2020)*. <https://gtnr.it/3ssF5IH>.

create new data pipelines and an infrastructure that supports AI-enabled processes). Those planning to use industrial AI to enable digital transformation should aim for at least level 4, with an IIoT system infrastructure that supports AI-enabled processes and AI trained staff in the field.

IIoT systems have long lifecycles (decades for example). This is longer than the time an AI technology needs to reach the required levels of readiness and maturity to be applied within an IIoT system in an effective manner.

The decision to use a particular AI technology in an IIoT system should be based both on short-term readiness and maturity, and on medium and long-term considerations. In some cases, the medium and long-term considerations may be the deciding factors in favor of using AI, with appropriate mitigation measures taken to cater for the initial period of lack of readiness and maturity.

3 USAGE VIEWPOINT

The primary consideration of the usage viewpoint is to address the concerns of stakeholders including business decision makers, technical managers, architects and plant managers about the expected usage of AI technology within an IIoT system. This is represented as sequences of activities involving human or logical users that deliver the intended functionality and ultimately achieve the fundamental system capabilities, as shown in Figure 3-1.

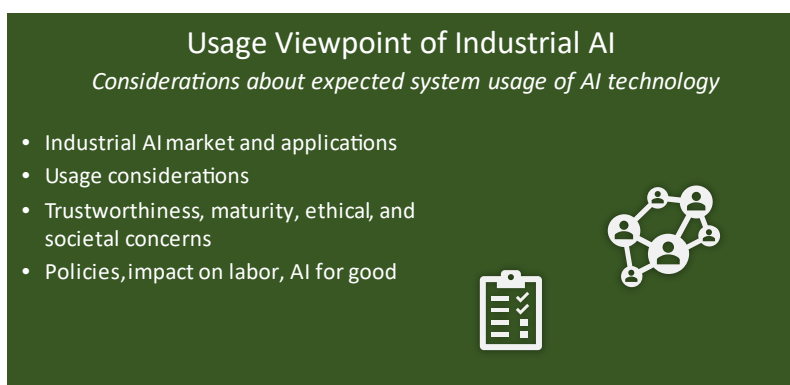


Figure 3-1. Industrial AI Framework Usage Viewpoint and Its Stakeholders. Source: IIC.

This section encompasses the usage of AI technology and that of AI-enabled IIoT systems. It provides an overview of the AI market and provides examples of use cases in industry in which AI added unique capabilities to the overall solution. It also discusses AI-related topics such as trustworthiness, ethics, explainability and societal considerations about AI usage in industry.

3.1 INDUSTRIAL AI MARKET

AI has been adopted into countless applications in industry with a wide range of applications such as predictive maintenance, quality inspection and assurance, supply chain optimization, equipment condition-based monitoring and manufacturing process optimization. Refer to Annex B for exemplary use cases of AI in industry.

In 2019, the IoT Analytics firm predicted that “By the end of the year, the Global Industrial AI market is estimated at just under \$15B and expected to grow at 31% annually to become a \$72.5B market by 2025.”¹³ Global Market Insight, a market research firm, has projected that the global market size for AI in manufacturing will reach \$16 billion by 2025¹⁴, registering a 45% annual growth. This market covers things like GPUs, machine learning technology, computer vision technology, powerful AI chips at the edge and AI platforms with pre-built algorithms.

The possibilities for AI and the broad market are endless, however, there are concerns like trustworthiness, ethics etc. that may affect adoption (and how quickly implementations can be done). These concerns may vary from application domain to another as well as between use cases within an application domain even as far as reusing an AI system for a new implementation within the same use case. What creates these challenges is the learning nature of AI technology and the impact this has on training and other aspects.

3.2 USAGE CONSIDERATIONS

Industrial AI use cases are abundant¹⁵ in the industry, covering monitoring, optimization and control functions. Use cases include predictive maintenance, factory automation, supply chain management, fault detection and fleet logistics.

Table 3-1 shows a set of key roles that AI plays in many industrial AI applications:

Role of AI	Description
 Digitize/Extract/ Transform	Digitize, extract, transform raw data for analysis, sharing, archiving or distribution. Examples: • identify components (e.g. pump, valve) and their interconnection from plant engineering drawings and • extract key data points from medical charts.
 Analyze/Detect/ Diagnose	Analyze the data—typically to identify anomalies. Examples: • identify cancerous cells in MRI images, • identify product defects from images and • identify leakage from captured pipe's acoustics.
 Optimize	Tune a set of parameters to find an optimum point/output. Examples: • optimize the configuration of a coal-based power generator based on the type of coal used, • identify the placement of checkpoints to optimize traffic and • given a set of drop-off points, identify optimum travel routes. This is often done through <i>reinforcement learning</i> . ¹⁶

¹³ IoT Analytics: Industrial AI Market Report (2020-2025). <https://bit.ly/3JXSzVr>.

¹⁴ Global Market Insights: *AI in Manufacturing Market Size Worth \$16bn in 2025*. <https://bit.ly/3g67Gyr>.

¹⁵ McKinsey: *Notes from the AI Frontier: Applications and value of AI deep learning*. <https://mck.co/3k4qIMe>.

¹⁶ Refer to Annex A.

Role of AI	Description
 Generate	Given a set of parameters, generate acceptable solutions. Examples: • produce various design of a product given a set of examples and requirements, • identify known products that can be produced given the available materials and resources and • given a set of requirements, generate possible configurations of an assembly line. This is typically done through the use of <i>generative adversarial network (GAN)</i> – see reference above.
 Prescribe	Given a set of events/data points, prescribe the next course of action. Examples: • provide suggestions on how to reduce wear-and-tear of an equipment given its historical use and • provide suggestions on what equipment and tools to bring to a repair job.
 Predict	Use historical data to predict the likelihood of future events. Examples: • given the historical data, predict the likelihood an equipment will fail in the next 90 days (aka predictive maintenance) and • given the historical use, identify the likelihood a section of a floor will be occupied in the next two hours.
 Do/Act	Identify an appropriate action given a condition. Examples: • navigate a vehicle from point A to point B following a set of rules and avoiding obstacles and • navigate the movement of a robotic arm to pick item from a shelf.

Table 3-1. Key Roles of AI in Industrial Applications.

Numerous publications describe the enabling role of AI technology in IIoT systems.¹⁷ (Refer to the exemplary use cases in Annex B and the enabling role AI plays in these use cases.) AI has specific philosophical and adoption-related usage properties. On the philosophical side, we must ensure that any new or resulting concerns about AI and its properties are properly addressed. On the adoption side, there are three areas of consideration: trustworthiness, ethical and societal concerns, and policy considerations. Here, the decision to deploy or not deploy an AI-enabled industrial IoT system must be based on the level of assurances about these considerations and the specifics of the use case.

Unlike traditional IT systems where the addition of a capability or feature may enhance the service, an AI based system may change the fundamental assumptions and overall behavior. For instance, the learning nature of the system and the dependence of the outcome on the data may affect the trustworthiness of the system.

¹⁷ McKinsey: *Notes from the AI Frontier: Applications and value of AI deep learning*. <https://mck.co/3k4qIMe>.

Therefore, organizations may want to adopt a comprehensive risk management approach that can be tailored to the specific application, organization and needs. ISO/IEC DIS 23894¹⁸ (under development) is an example that builds on the generic ISO 31000¹⁹ Risk Management framework.

3.3 TRUSTWORTHINESS

The IIC defines the trustworthiness of IIoT systems^{20, 21} as the *degree of confidence that an IIoT system performs as expected with characteristics including safety, security, privacy, reliability, and resilience in the face of environmental disturbances, human errors, system faults and attacks*. System design needs to consider the interactions of the characteristics and the associated tradeoffs.

The concept of trustworthiness of IIoT systems is directly related to the convergence between the concerns related IT systems and those related to OT systems. Refer to Figure 3-2.

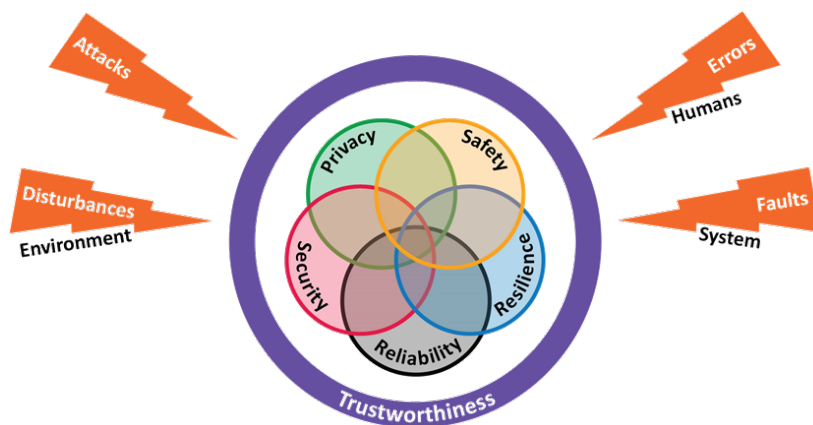


Figure 3-2. Trustworthiness of IIoT Systems. Source: IIC.

Trustworthiness concerns must be addressed throughout the lifecycle journey of the IIoT system and not only at the time of its design or implementation.²²

There is a direct relationship and interdependence between the quality of the implementation of the AI system and the trustworthiness of that system. If the AI is implemented in an unprincipled manner, the weaknesses may increase risks related to safety, security, privacy, reliability and resilience of the system.



In the energy sector, AI is used heavily in predictive maintenance applications. Weaknesses²³ in the predictive maintenance AI model may reduce its effectiveness

¹⁸ ISO/IEC DIS 23894: Artificial intelligence — Risk management. <https://bit.ly/3DI7pRb>.

¹⁹ <https://www.iso.org/iso-31000-risk-management.html>

²⁰ IIC: *Industrial Internet Trustworthiness Framework Foundations*. Refer to Annex C for details.

²¹ IIC: *Journal of Innovation: Trustworthiness*. Refer to Annex C for details.

²² Please refer to the “Managing Trustworthiness as an Iterative Process” discussion (Section 2.2) in IIC’s *Industrial Internet Trustworthiness Foundation Framework* (referenced earlier in this document).

²³ Data bias, training, testing, security, etc.

Example | in its role in pipeline inspection and leak detection.²⁴ This can lead to significant safety and operational issues.²⁵

From the AI perspective, it is important to augment existing standards, best practices and frameworks to ensure that users can trust AI-enabled IIoT systems. This has implications on established disciplines like security and privacy, as well as safety, reliability and resilience.

These challenges are compounded by the inherent interdependency between the different characteristics of IIoT trustworthiness. A weakness in one characteristic may negatively affect another characteristic. For example, a weakness in the security may lead to safety violations.

A systematic approach to risk management is needed to ensure that the system is trustworthy. This in part due to the nature of AI systems as the behavior can change due to a variety of factors such as adaptive learning algorithms,²⁶ training data and variations of operational data.

3.3.1 SECURITY

Securing²⁷ an IIoT system must be based on the same principles, standards, and best practices that apply to IT and OT systems. Examples of such standards include the ISO/IEC Joint Technical Committee (JTC1) ISO/IEC 27000²⁸ family of Standards for IT systems and the IEC Technical Committee 65 (TC 65) IEC 62443²⁹ for operational technology in industrial and critical infrastructure.

For an AI-enabled IIoT system, one must also consider the additional security concerns for the AI system itself, its data and its training ecosystem. In addition, the unique requirements necessitated by IT/OT convergence and the interdependence between OT concerns and IT concerns must also be addressed.³⁰

AI is a data-driven technology. In an AI-enabled IIoT system, more operational data is stored and consumed, especially if the AI is running on an edge device. Thus, adding AI to an IIoT system can increase the organization's vulnerability to cybersecurity threats. Generally speaking, security breaches are hard to detect with AI systems. If an actor manages to compromise the AI or replace it with a system that has loopholes, there can be new and unexpected security threat vectors, with significant impact on the overall system.³¹

²⁴ Leak detection imaging systems use AI to process images and detect, confirm, or reject potential leaks.

²⁵ Cost-effectiveness, productivity, worker risk, etc.

²⁶ Refer to Annex A.1.

²⁷ For more information about the topics of security and trustworthiness in IIoT systems, please refer to the following IIC documents (referenced in Annex C): Industrial Internet Security Framework (IISF), IoT Security Maturity Model (ISMM) and IIoT Trustworthiness Framework Foundation (IITFF).

²⁸ ISO/IEC 27000 <https://webstore.iec.ch/publication/62675>

²⁹ IEC 62443 <https://webstore.iec.ch/publication/7030>

³⁰ Refer to the trustworthiness discussion in Section 3.3.

³¹ For example, flawed false positive and false negative characteristics and compromised performance.

When designing an AI system and integrating it into an IIoT system, it is important to understand:

- which assets need to be secured,
- what are the related data governance models,
- what controls are needed to ensure that the AI systems are secure and
- what are the broader considerations for data protection in relation to AI,³² including governmental and regulatory requirements for data privacy and confidentiality.

Section 7 of the IISF document identifies the functional building blocks of IIoT system security (Figure 3-3) and describes the common data protection functions that encompass data-at-rest in the endpoints, data-in-motion in the communications, and all data gathered as part of monitoring and analysis functions and all the system configuration and management data.

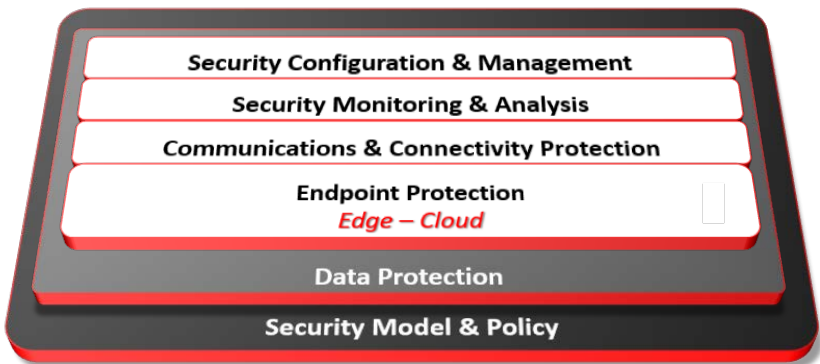


Figure 3-3. Security Framework Functional Building Blocks. Source: IIC IISF.

To secure AI systems, organizations need to understand these security functional building blocks and address the AI-specific security considerations across them. Refer to Table 3-2 below:

IIoT Security Functional Building Blocks	Securing AI systems
<i>Endpoint protection</i> implements defensive capabilities on devices at the edge and in the cloud. Primary concerns include physical security functions, cybersecurity techniques and an authoritative identity.	Endpoint protection requirements must be extended to the AI systems embedded within the endpoints (for example, remote security cameras that include AI-based image recognition capabilities).
<i>Communications and connectivity protection</i> uses the authoritative identity capability from endpoint protection to implement authentication and authorization of traffic. This includes cryptographic techniques for integrity, confidentiality and data flow control techniques.	Data produced and consumed by AI systems must be protected while in transit (in-motion) using the same methods as sensor data and actuator command data.

³² In IIoT systems that process sensitive data (healthcare, financial services, security and more), the AI systems must also secure and protect this sensitive data.

IloT Security Functional Building Blocks	Securing AI systems
Once endpoints are protected and communications secured, the system state must be preserved throughout the operational lifecycle by <i>security monitoring and analysis</i> and controlled <i>security configuration and management</i> for all system components.	These security measures must be extended to the AI systems and the data they produce and consume, throughout the operational lifecycle of the IloT system.

Table 3-2. Securing Industrial AI Across the IloT Security Function Building Blocks.

During implementation, the general security design principles that guide the capabilities and techniques employed in implementing security in IloT systems (based on Saltzer and Schroeder³³) must also be applied to AI security:

- Principle of economy of mechanism: keep the design as simple and small as possible.
- Principle of fail-safe defaults: base access decisions on permission rather than exclusion.
- Principle of complete mediation: access to every object must be checked for authority.
- Principle of open design: mechanisms should not depend on the ignorance of potential attackers, but rather on the possession of specific and more easily protected keys.
- Principle of separation of privilege: where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.
- Principle of least privilege: every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- Principle of least common mechanism: minimize the amount of mechanism common to more than one user and depended on by all users.
- Principle of psychological acceptability: the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

Example Reports about Industrial AI Security

The ENISA AI Cybersecurity Challenges report³⁴ provides further discussions about AI and security. The report states that AI and cybersecurity have a multi-dimensional relationship and interdependencies between them:

“Cybersecurity for AI: lack of robustness and vulnerabilities of AI models and algorithms, e.g. adversarial model inference and manipulation, attacks against AI-powered cyber-physical systems, manipulation of data used in AI systems, exploitation of computing infrastructure used to power AI systems, data poisoning, environment variations which cause variations in the intrinsic nature of the data, credible and reliable training datasets, algorithmic validation / verification (including the integrity of the software supply chain), validation of training and

³³ Saltzer, Jerome H and Schroeder, Michael D.: The Protection of Information in Computer Systems (Fourth ACM Symposium on Operating System Principles). <http://www.cs.virginia.edu/~evans/cs551/saltzer/>.

³⁴ European Union Agency for Cybersecurity: AI Cybersecurity Challenges. <https://bit.ly/3yUscK7>.

performance evaluation processes, credible and reliable feature identification, data protection / privacy in the context of AI systems, etc.

AI to support cybersecurity: AI used as a tool/means to create advanced cybersecurity by developing more effective security controls (e.g. active firewalls, smart antivirus, automated CTI (cyber threat intelligence) operations, AI fuzzing, smart forensics, email scanning, adaptive sandboxing, automated malware analysis, automated cyber defence, etc.) and to facilitate the efforts of the law enforcement and other public authorities to better respond to cybercrime, especially the criminal misuse of AI.

Malicious use of AI: malicious/adversarial use of AI to create more sophisticated types of attacks, e.g. AI powered malware, advanced social engineering, AI-augmented DDoS attacks, deep generative models to create fake data, AI-supported password cracking, etc. This category includes both AI-targeted attacks (focused on subverting existing AI systems in order to alter their capabilities), as well as AI-supported attacks (those that include AI-based techniques aimed at improving the efficacy of traditional attacks)."

3.3.2 PRIVACY

Data privacy regulates how personal data (also referred to as personally identifiable information or PII³⁵) should be handled, what types of actions are permitted on that data, and who is authorized to carry out these actions. Data privacy laws are proliferating in various jurisdictions³⁶ and are becoming increasingly stringent. As with security, addressing the privacy concerns in AI-enabled IIoT systems must be based on the same privacy principles, standards and best practices that apply to IT and IIoT systems, and must consider the additional privacy concerns that the AI system, its data and its training ecosystem introduce.

Many new cars have in-car cameras to provide additional safety and comfort to the passengers. These cameras can help detect sleepy or distracted drivers.³⁷ However, these same cameras and the AI algorithms that process their output can also be used to capture the demographic of the passengers (e.g. skin color, language used), habits (drinking while driving) and mental health issues.³⁸ Even though the car owner or its driver may have given their consent to turn on their in-car cameras, it does not mean that the manufacturers and service providers of these cars have the right to analyze the data to gain insight that deviate from the original intention of gathering the data, which is driver safety. This type of consent is referred to as *informed consent*.³⁹

³⁵ US GPO Privacy Program: *Privacy 101, Awareness and Best Practices*. <https://bit.ly/3smsgzr>.

³⁶ GDPR in the EU, CCPA in California, PIPEDA in Canada.

³⁷ NY Times: *Sleepy Behind the Wheel? Some Cars Can Tell*. <https://nyti.ms/3ssDx1l>.

³⁸ ResearchGate: *Eye movement analysis for depression detection*. <https://bit.ly/3m6HjfO>.

³⁹ Accenture: *Informed Consent and Data in Motion*. <https://accntu.re/3k3s3h0>.



Example

A prime example of privacy controls is the EU General Data protection Regulation⁴⁰ (GDPR), which imposes a wide range of restrictions and controls on the capture, usage, and retention of personal data. The GDPR is consequential for AI applications that process personal data. In particular, Article 22 limits the right of data controllers⁴¹ to do profiling and make decisions about a data subject “based solely on automated processing” where those decisions have legal or similarly significant effects on the individual.⁴² This implies that AI-enabled applications⁴³ that handle personal data are also subject to data protection requirements.

Informed consent, security, transparency and accountability about what data is captured and how it will be used are key facets in maintaining trust between manufacturers and customers.

For some IIoT systems, an additional step that can be done to strengthen customers’ trust is *direct auditability*. When data is captured directly from the equipment without a human in the loop, it is possible to incorporate auditability directly into the system. This means capturing data from the sensors and detailed steps in the decision-making process (i.e., data lineage)—and making this data available to a review or audit board.

3.3.3 CONFIDENTIALITY

AI operates in a data-intensive environment. Broadly speaking, confidentiality raises two areas that have to be addressed. First, there may be situations where confidential data cannot be mixed with non-confidential or other confidential data whether it is operational or training data. Second, care must be taken that insights provided by the AI system based on confidential data cannot be used to infer the source data used. Mechanisms must be put in place to address the confidentiality of business and commercial data.

For instance, with IIoT devices, manufacturers of advanced equipment—from MRI scanners to jet engines and stamping machines—may use AI-enabled pay-per-use capabilities for fine tuning and optimization and predictive maintenance. Sensors can monitor equipment such as how often they run, how long, the peak and sustained workloads. Because this information can provide insight about business activities that have a sensitive nature, customers may wish to keep this information confidential.

There are also situations where it may be possible to extract personal data from was initially considered to be business and operational data, for example, AI-powered facial recognition on

⁴⁰ EU LEX Europa: *GDPR Regulation*. <https://bit.ly/3iPTNXc>.

⁴¹ The party that determines the purposes for which and the means by which personal data is processed. *European Commission Rules for Business and Organizations*. <https://bit.ly/2Uoa1gG>.

⁴² Example: Limit the right to vote in an election, deny a particular social benefit provided by law (child or housing benefit), negatively affect financial circumstances (eligibility for credit), and many others.

⁴³ Example: Patient-related data in healthcare, worker-related data in manufacturing, etc.

the shop floor. In these situations, the data and insight extracted from it may be also subject to data privacy controls.

3.3.4 EXPLAINABILITY

How can an AI system be trusted if it is not understood? This question is at the forefront of many AI discussions because it will directly affect adoption and must be dealt with upfront.

Understanding an AI system can have two perspectives that relate to the context of use of the AI system within the specific IIoT application. First, from a systems integration perspective, an IIoT system that will incorporate AI needs to understand how the AI system works including its predictive nature so that the overall system can be defined, architected and designed. Second, for the end-user of the AI-based IIoT service, a level of understanding about what the AI component is doing is necessary to build trust in the system and its insights. For instance, this can include a non-technical explanation of the system, bounds of what the AI can and cannot do, how the AI uses data and any standards used in the design of the AI system (example: a management systems standard; see section 6.3).

For instance, unlike other IT systems, AI is a learning and predictive system that depends on data. Traditional verification and system design around AI systems may not be feasible, so proper safeguards must be put in place to avoid undesirable outcomes when the AI goes wrong. Explainability and understanding of the AI system are essential to implement such safeguards.

Another example is that many machine learning algorithms—especially those with deep learning—are black-boxes that can make decisions (e.g. determine whether a picture is of a pedestrian). To build trust in the system, the AI development and IIoT provider should indicate broadly how the AI insights are reached.⁴⁴



The application of AI in IIoT systems requires technology-specific considerations related to explainability. In this context, explainability of AI is a direct result of the nature of AI technology.

3.3.5 CONTROLLABILITY

Controllability is a fundamental security and safety concern with AI-enabled IIoT systems. However, it has not been proven yet that controllability of AI will always be fully achievable.⁴⁵ This is because the problem has many sub-types and can lead to inherent ambiguity.

Take for example the potentially different scenarios of an industrial AI that issues a command (rather than provide analytics-based recommendations): “Stop the line when a potential irregularity has been detected”:

- Explicit control: the AI may stop the line immediately, even in the middle of an operation.

⁴⁴ Example: why a client was denied insurance.

⁴⁵ Yampolskiy: *On Controllability of AI*. <https://bit.ly/3xT9W2l>.

- Implicit control: AI tries to stop the line at the first safe opportunity.
- Aligned control: AI relies on its model of human intentions behind the command and uses common sense interpretation of the command to do what a human hopes will happen.
- Delegated control: AI stops the process without waiting for a human to issue a command if it believes that the process can benefit from an enhancement.

3.4 ETHICAL AND SOCIETAL CONCERNS

The context of the use of AI technology has a wide range of concerns relating to ethics, societal concerns, bias, safety, impact on labor and policy in general.

3.4.1 ETHICS

The goal of this section is to highlight some of the key ethical issues when applying AI in an industrial environment, namely privacy, biases and inadvertent algorithmic consequences. It does not replace or summarize numerous studies⁴⁶ on the topic, such as automated industrial equipment optimization,⁴⁷ energy usage prediction⁴⁸ and cancer detection.⁴⁹

AI must be used responsibly to avoid unintended consequences. In privacy for example, implementing informed consent in an AI-enabled system (see section 3.3.2) may not guard against advances in AI that may in the future be capable of inferring personal information from data that was deemed before to be compliant with privacy controls.

A growing number of countries have issued guidelines and principles for AI ethics. Table 3-3 below is an example of AI ethics framework issued by a government agency, in this case, the Department of Industry, Innovation and Science, Energy and Resources in Australia.⁵⁰

AI Ethical Principle	Description
1. Human, social, and environmental wellbeing	Throughout their lifecycle, AI systems should benefit individuals, society, and the environment.
2. Human-centered values	Throughout their lifecycle, AI systems should respect human rights, diversity, and the autonomy of individuals.
3. Fairness	Throughout their lifecycle, AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities, or groups.
4. Privacy protection and security	Throughout their lifecycle, AI systems should respect and uphold privacy rights and data protection and ensure the security of data.

⁴⁶ Inventory Algorithm Watch: AI Ethics Guidelines Global Inventory. <https://bit.ly/2Xq8E26>.

⁴⁷ Bosch Center for AI: *Control Optimization Through Reinforced Learning*: <https://bit.ly/37PR6yu>.

⁴⁸ NIST: *Towards Statistical Modeling and ML Based Energy Usage Forecasting in Smart Grid*: <https://bit.ly/3CWd9BO>.

⁴⁹ Science Daily: *Man against machine: AI is better than dermatologists at diagnosing skin cancer*: <https://bit.ly/3g9Ff2Q>.

⁵⁰ Australian Government: *AI Ethics Principles*. <https://bit.ly/3CWt5UQ>.

AI Ethical Principle	Description
5. Reliability and safety	Throughout their lifecycle, AI systems should reliably operate in accordance with their intended purpose.
6. Transparency and explainability	There should be transparency and responsible disclosure to ensure people know when they are being significantly impacted by an AI system and can find out when an AI system is engaging with them.
7. Contestability	When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or output of the AI system.
8. Accountability	Those responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.

Table 3-3. Core Principles of the AI Ethics Framework. Source: Department of Industry, Australia.

3.4.2 BIAS

Many applications of AI provide insights that are intended for decision making. In predictive maintenance for example, AI is used to determine whether a particular part is likely to break within a certain period. For machine optimization, it can be used to set certain machine configurations (e.g. fan speed, fan run time) to optimize certain parameters (e.g. energy usage).

Decisions made by AI are based on learning models that are trained with data sets. Ensuring that appropriate training data is used in model training is critical to the overall quality of the algorithm and the decisions it makes. If there is unintended bias in the training data set, the decisions made by the AI models will have biases. Let us illustrate this by an example. Suppose we are to develop a ML application to predict mean-time-to-failure (MTTF) of a temperature-sensitive valve of an outdoor pump. The machine learning model is trained with data captured from existing pumps. However, for the model to do an acceptable job in predicting MTTF, the training data must represent the right conditions.

Without a carefully designed process, biases may be introduced throughout the entire data supply chain—from the source to model training to the application:

Biases in training data: Suppose the training data was captured from pumps operating when the weather is warm. The resulting model might not accurately predict valve's MTTF in cold weather.

Biases during model training: Often, to speed up the training time, only a subset of the captured data is used. However, the subset must be carefully curated to represent the overall captured data fairly—otherwise, bias may be introduced. If, for example, the subset contains more data captured during warm weather than cold, this imbalance may result in an inaccurate model.

Biases due to human nature: Special attention must be made on data from human's actions or decisions. There are well-known studies that humans' unconscious biases are quite pervasive in

their decision-making process.⁵¹ If we are to create an automated decision-making application that is trained based on the decision made by a human, a special step needs to be taken to check—and ideally remove—unintended biases from the underlying data.⁵² Otherwise, the resulting model and the application will embed these unintended biases. As more people use this application, the impact of these biases is amplified.

Biases introduced during operation: Unintended biases can be introduced during normal operation, based on the operational data that the AI encounters. In such cases, a retraining of the AI system is needed.

3.4.3 SAFETY

Safety is a well-established discipline with standards and well-defined best practices that cover the full lifecycle of systems from design to implementation, deployment, operation, and final decommissioning. IEC 61508⁵³ and IEC 61511⁵⁴ are examples of such safety standards.

AI safety is defined as the reduction of risks posed by AI, especially when the AI computation outcome can be applied directly back to the physical world. The impact of AI on the safety functional and integrity requirements must be considered and addressed throughout the full lifecycle of the AI system and the IIoT system with which it is integrated: planning, design, implementation, and operation.

Given AI's automated and "hands-off" nature and nearly incomprehensible potential, safety concerns can be significant. Organizations should mitigate industrial AI risk and bias to reduce the possibility of unintended harm or loss of life. "Accidents" due to unintended oversights in information processing and decision-making are also a true possibility—executive leaders and business managers should be aware of how such accidents can occur.



Note

AI safety must be considered throughout the lifecycle of AI strategic planning, implementation and usage, especially from a preventative point of view. Given the potentially irreversible negative consequences of "rogue AI", organizations need to ensure they have strong internal controls surrounding their AI environment starting with the planning stage.

As organizations progress with their AI initiatives, it is important to consider the "black box" perception that may exist around AI models. It is easy to see the inputs and outputs of the AI model, but it may be difficult to understand how the model works (such as the technology involved or decision-making mechanisms at play) and build controls for the model itself.

⁵¹ Harvard Business Review: *What we do about the biases in AI?* <https://bit.ly/3g73zm4>.

⁵² The Next Web: *How to detect unwanted bias in machine learning models.* <https://bit.ly/2UoafV4>.

⁵³ Functional safety of electrical/electronic/programmable electronic safety systems: IEC 61508. <https://bit.ly/3iTNPEF>.

⁵⁴ Instrumented systems for the process industry sector: IEC 61511. <https://bit.ly/3yXLWfC>.

Lastly, within an AI initiative, there needs to be multiple feedback loops and an iterative approach to development and continuous improvement to maintain realistic expectations, ensure transparency and learn from lessons along the way.

Defense line #1 revolves around security expectations for authentication and authorization. Role-based administration and control prevents an unauthorized actor from manipulating industrial AI data, devices or processes.

Defense line #2 is provided by the data management expectations for information models, which reduces the unintended consequences of ad hoc configurations of system components. A common representation of attributes enables simpler industrial AI application design and realizations that business owner can verify and validate.

Defense line #3 considers connectivity expectations for reliable data synchronization. Missing or incomplete data sets could contribute to out-of-bound algorithms.

Defense line #4 deals with oversight of post-process AI results—confirming that they are within expected ranges and engage human judgement to review and analyze anomalies.

When applying industrial analytics, and interpreting and acting on the result, strong safety requirements must be in place safeguarding the wellbeing of the workers, users and the environment. Industrial AI must satisfy a higher level of accuracy in its analytic results. Any system that interprets and acts on the results must have safeguards against undesirable and unintended physical consequence.

Furthermore, industrial operations deal with the physical world and industrial analytics needs to be validated with domain-specific subject matter expertise to model the complex and causal relationships in the data. The combination of first principles, e.g. physical modeling, along with other data-science statistical and machine-learning capabilities, is required in many industrial use cases to provide accurate analytics results.

3.5 IMPACT ON LABOR FORCE

Recent news and reports⁵⁵ warn that advances in AI have the potential to disrupt labor markets by creating job displacements.⁵⁶ AI and automation can augment the productivity of some workers and it will likely transform almost all occupations to some degree.

There will definitely be some impact of AI on the job market, but not all jobs are equally affected.

- Jobs that are repetitive and relatively straight forward to perform are the most affected, (example: assembly workers on production lines, and operators of equipment and vehicles with AI-powered autonomous capabilities (cranes, trucks, etc.)).

⁵⁵ Example: PNAS – *Towards understanding the impact of AI on labor*. <https://bit.ly/2VYuwkx>.

⁵⁶ Many AI applications target non-labor cost savings, example minimizing energy consumption in a factory.

- Jobs that require plenty of interpretation and judgement are slower to be automated (example: healthcare workers whose job requires soft skills and the ability to connect with patients, and engineers and data scientist who need to design and optimize processes).
- AI is not simply about automation and replacing people. AI can make existing workers more productive—by having AI performing mundane and boring tasks and focusing the workers on higher-value tasks (example: using AI to schedule nurses in a hospital so that nurses can focus on caring for patients).
- With more automation being introduced, there will be more jobs related to fixing and improving the automation (example: fixing robots and machines).
- There will also be new types of jobs introduced as well, such as data quality, governance, and ethicians.

Despite the mix of upsides and downsides, the rising impact of AI on automation is raising fears of mass technological unemployment and a renewed call for policy efforts to address the consequences of technological change.

To do that, organizations must overcome the barriers that inhibit scientists from measuring the effects of AI and automation on the future of work, especially those related to the lack of high-quality data about the nature of work, (e.g. the dynamic requirements of occupations), lack of empirically informed models of key microlevel processes (e.g. skill substitution and human-machine complementarity) and insufficient understanding of how cognitive technologies interact with broader economic dynamics and institutional mechanisms (e.g. urban migration and international trade policy).

Organizations must also address the issues related to ethics and fairness as they relate to the effect of AI automation on the labor force. This can be a real differentiator in the marketplace where reputation and ethical values are as important as delivering products and services.

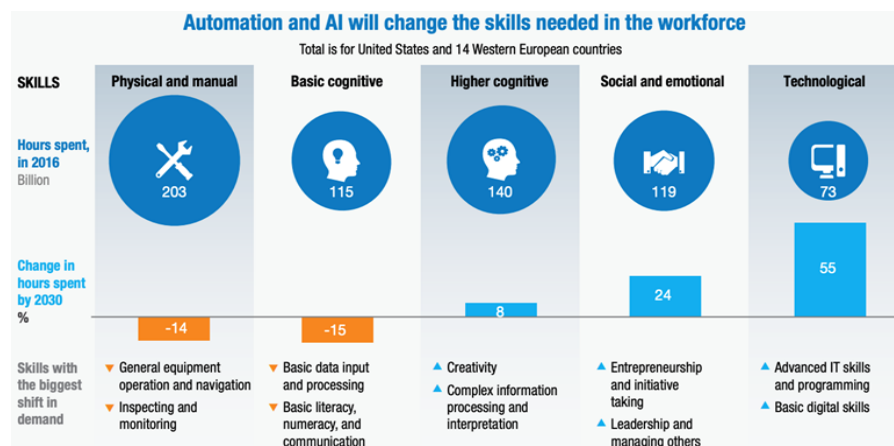


Figure 3-4. Skill shift: Automation and the Future of the Workforce. Source: McKinsey.

McKinsey's report about AI's impact on labor⁵⁷ confirms the above and states that automation and AI will change the skills needed in the workforce (see Figure 3-4). The report makes several labor assertions related to AI, such as:

- Demand for digital and technological skills will grow by 55% by 2030.
- Demand for social and emotional skills such as leadership and managing others will rise.
- Demand for higher cognitive skills will grow moderately overall, but will rise sharply for some of these skills, especially creativity.
- Some skill categories will be less in demand. Basic cognitive skills, which include basic data input and processing, will decline.
- Demand for physical and manual skills, which include general equipment operation, will drop but will remain the largest category of workforce skills in 2030 in many countries.
- Governments will need to strengthen safeguards for workers in transition and encourage mobility, including with a shift to portable benefits.

3.6 REGIONAL AND INDUSTRY-SPECIFIC CONSIDERATIONS

Regions will make decisions about the deployment and use of AI in particular applications based on some of the issues introduced, such as trustworthiness, impact on labor force and unintended bias. This may come in the form of legislation that leverages international standards and guidance from industry consortia. Industries may do the same to develop their specific AI roadmap, guidance and standards.

3.7 AI AS A FORCE FOR GOOD

Organizations must maintain a balanced view between the significant benefits of AI technology and its risks. They must also persist in their efforts to mitigate these risks.

In addition, AI is playing an enabling role in a growing number of solutions that advance the state-of-the-art towards “for good” goals, as opposed to “for profit”. This is evidenced by the growing use of AI in use cases and applications in the industry, such as good health and wellbeing, affordable clean energy, sustainable cities and climate action.

⁵⁷ McKinsey (2018): *Skill shift: automation and the future of the workforce*. <https://mck.co/3xYoQ7f>.

4 FUNCTIONAL VIEWPOINT

The functional viewpoint (Figure 4-1) focuses on the functional components in an industrial AI system, its structure and interrelations, and the relation and interactions of the system with external elements to support the usages and activities of the overall system.

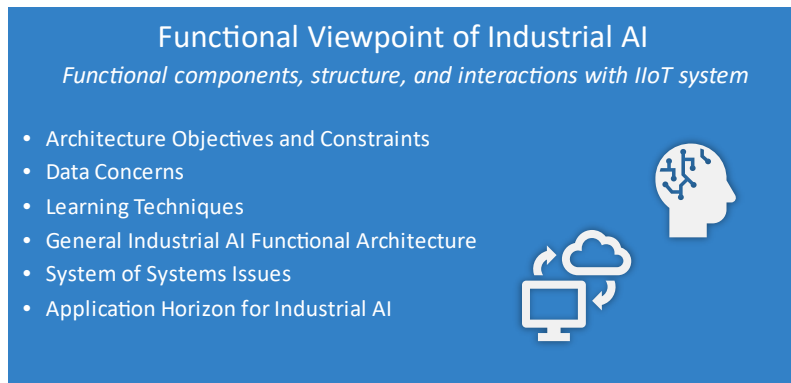


Figure 4-1. Industrial AI Framework Functional Viewpoint and Its Stakeholders. Source: IIC.

4.1 ARCHITECTURE OBJECTIVES AND CONSTRAINTS

The discussion of functional components of industrial AI needs to be based upon a basic understanding of the process in which the industrial AI models are built and used. An AI model is a single or a set of computer programs implementing algorithms to solve specific problems.

One key characteristic of AI models is their ability to learn from data. Tom M. Mitchell gave a classical definition of learning in computer program:⁵⁸ *“A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T , as measured by P , improves with experience E .”*

Here in the context of our discussion, experience is contained or manifested (evidently or hidden) in data that we captured from a certain context or environment. The process to make use of AI, or more specifically machine learning models, typically involves two major phases, model building and model execution (use), as illustrated in Figure 4-2.

In the model-building phase, one is to create and verify the models for a specific problem domain from data gathered from the real environment.⁵⁹ In the model-execution phase, the resulting models from the model-building phase can then be deployed into a system to be executed over data from the real environment (the runtime) to detect patterns and perform predictions. In this phase, various algorithms may be explored, sometimes a group of algorithms are put together in conjunction or in an ensemble to give the best result.

⁵⁸ Tom M. Mitchell at Carnegie Mellon, Machine Learning (McGraw-Hill International Editions Computer Science Series), 1997, ISBN-10: 0071154671.

⁵⁹ Though in some cases, some of the data could be initially simulated.

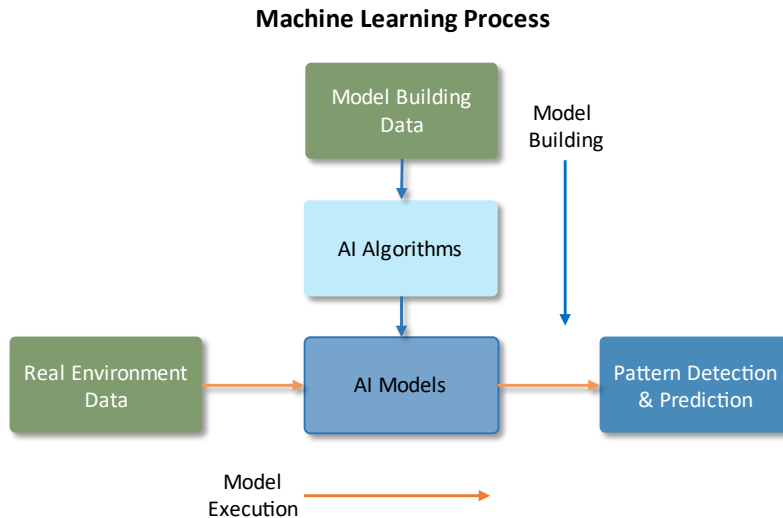


Figure 4-2. AI/Machine Learning Model Process.

Model building is often an iterative process involving exploration algorithms, training, fine-tuning and verification of the models. Even after a model has been initially deployed in the runtime, it can be retrained with new data before an updated version of the same model can be redeployed into the runtime to increase its accuracy or to cover broader problem space or conditions.

In the model-execution phase, the execution of models can be done in a few modes depending on the nature of the problems it is designed to solve.

Ad hoc or on-demand, periodical batch execution: the models are run on demand triggered by some events or a timer. For example, in predictive maintenance, a model predicting machine maintenance needs can be run periodically, or when a substantial amount of data has been accumulated, e.g. when data arrives from an oilrig for detailed large-scale analysis.

Near-real-time execution: the models are run continuously as long as there are new data available. For example, models monitoring an industrial furnace in real time to detect operational anomalies may run continuously as long as data are collected from the furnace in operation.

4.2 DATA CONCERNS

Data are essential to both model building and execution. Data quality is important to both phases and the quantity of data is also crucial for building versatile models.

Data quality concerns several factors that may affect the quality of the models. These include:

- whether the data set used in model training contains (even hidden) features of patterns that are to be detected,
- whether features (even implicit) contained in the data set have a high enough signal to noise ratio and
- whether the data set contains systematic bias that would obscure model training.

Data quantity concerns deal with whether the data set is large enough so that:

- the data set covers sufficient problem space (range of variation in conditions, scenarios or situations) so that the models are robust enough to handle situations that would occur in the real environment in which the models are to be executed and
- the data set enables the models to be trained maturely (unlike the neural network in a human brain that has a strong ability of inference so that only a few examples are needed to learn to recognize a certain pattern, machine learning requires a large number of samples to form and cement its capacity of pattern recognition).

Refer to section 5.2.7 Data Properties for further details.

4.3 LEARNING TECHNIQUES

Due to the importance of data in AI and machine learning modeling, the process of enabling AI and machine learning is more complex than what was entailed in Figure 4-2. A more detailed representation is given in Figure 4-3, with some data processing stages added.

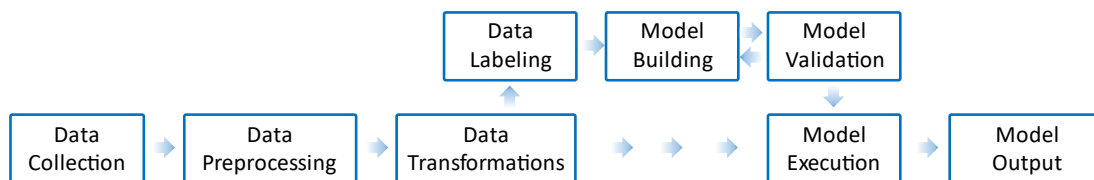


Figure 4-3. Data Processing for AI Modeling.

In the IIoT context,

- Data collection involves connecting to industrial equipment and sensors and collecting data from them.
- Data preprocessing involves data validation (type, range, consistency), conversion (e.g. units, time zone), alignment (e.g. timestamp), noise reduction (e.g. smoothing), missing data treatment and data thinning. The goal of data preprocessing is to ensure the data quality available for the next stage.
- Data transformation involves data processing that makes model building (including learning) more feasible. Common examples include transformation such as kernel trick and dimension reduction (e.g. PCA⁶⁰) so either to make the modeling more sensitive to the true underlined features of the data or to reduce the amount of processing during the learning to an economical level without degrading the final model outcome.⁶¹
- The processing steps in data preprocessing and data transformation must be consistent between the model building and execution phases to ensure the same data content and formation are input into the models during model training and validation and execution.
- Data labeling involves identifying data set based on its known features with meaningful labels to provide context so that the model can learn from the data set during training. Data labeling is required for supervised machine learning algorithms.

⁶⁰ Principal Component Analysis. <https://arxiv.org/pdf/1404.1100.pdf>.

⁶¹ Data transformation is sometimes considered part of the modeling.

Industrial IoT Artificial Intelligence Framework

- Model building involves the exploration and selection of adequate algorithms for the problem at hand and the training and fine tuning of the models with data sets available for learning.
- Model validation involves testing the model using validated data sets, which are data that are not used in the model training process
- Building and validation of models are an integral process that involves many iterations.
- Model execution involves the execution of the models in the real environment or using real-world data as input into the models to solve specific problems.
- Model output is the outcome of the model execution typically involves pattern recognition and prediction.

AI models cannot usually solve world problems just by themselves. On one hand, it is evident that the application of AI models heavily dependent on data both for its training and use for solving real-world problems. In the industrial context, it usually relies on some sort of IIoT platform to provide a set of data functions that include data collection, preprocessing, storage, query and management to provide data consistently for both training and execution.

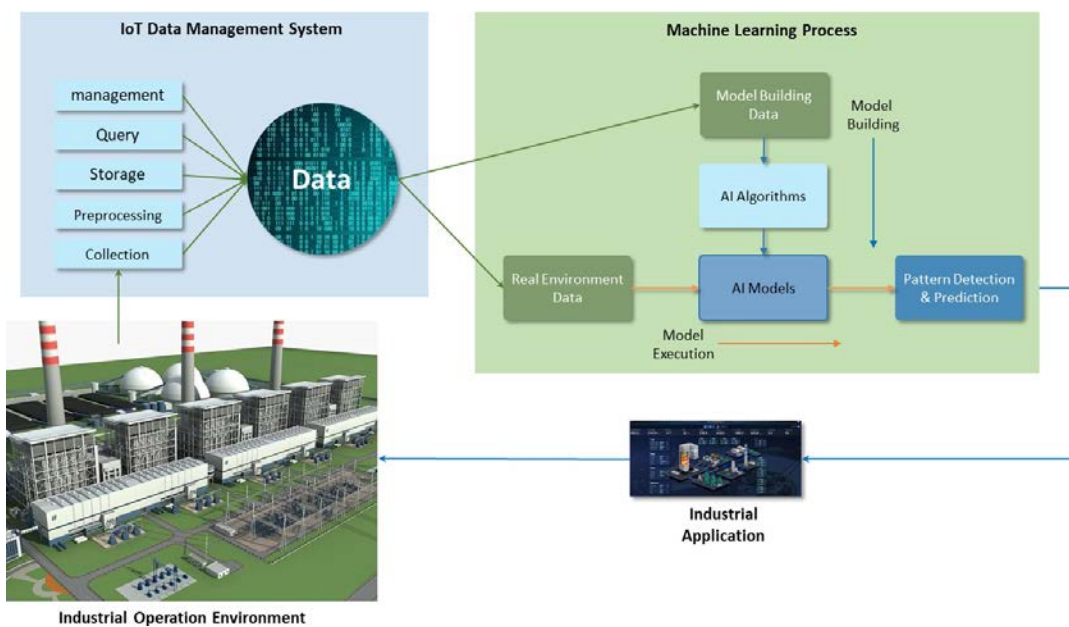


Figure 4-4. Industrial AI System.

On the other hand, the output of an AI model must combine with business logic or context to transform the insights from the models into actionable decisions. In turn, these decisions need to be acted upon, directly or indirectly, to optimize the operation of the industrial equipment and processes. The mechanism is typical through industrial domain applications. AI models and industrial domain applications are illustrated in Figure 4-4.

Relying on vast amount of data collected from the industrial operational environment, industrial AI, along with conventional models based on first principles and traditional statistical models, will support a new generation of data-driven and AI-driven smart industrial applications.

Industrial IoT Artificial Intelligence Framework

This forms a closed feedback loop in the industrial operation environment, to enable increasingly intelligent industrial operations through optimal business decisions, optimal operational processes and optimal equipment state, as illustrated in Figure 4-5.

The data collected include data about people (e.g. for worker safety), equipment, materials, processes, products and environment by IIoT systems.

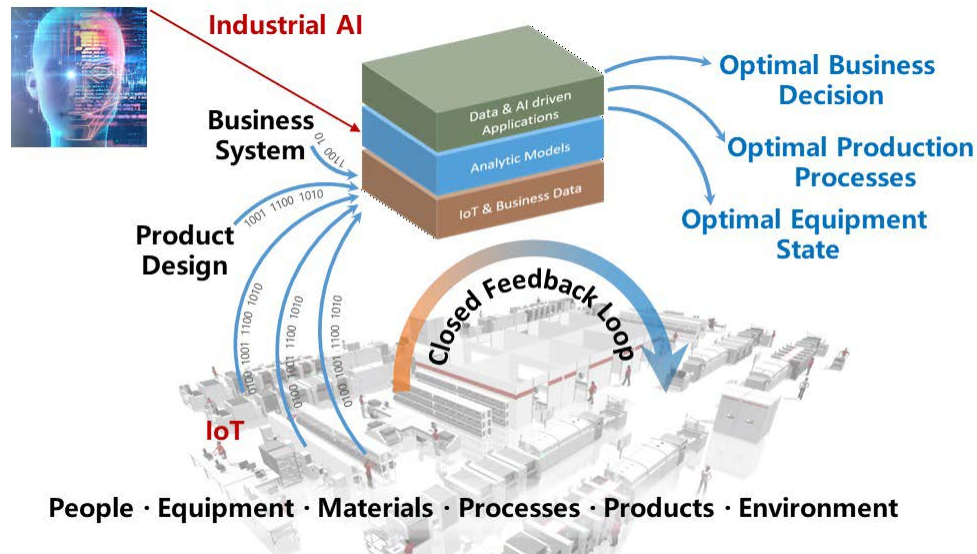


Figure 4-5. Industrial AI in Industrial Operation Environment.

4.4 GENERAL INDUSTRIAL AI FUNCTIONAL ARCHITECTURE

Industrial AI is a core functionality in a larger system enabling increasingly intelligent industrial operations. Industrial AI functionality relies on underlying services, such as data collection, cleansing, storage and access, runtime support for model building and execution, an integration framework and APIs to support industrial operational or business applications (Figure 4-6).

Data is foundational to industrial AI for both model training and model execution. For a given industrial application environment, data support to industrial AI is typically provided by some data platform for data collection, cleansing, storage, access and other data management functions.

The data platform provides historical and real-time basis for building and running AI models. When an AI model is built (including exploration, training, and validation) with historical data, typically in a model-building platform or environment, the resultant model is deployed in a runtime platform to be run with real-time data and in many cases with historical data as well, for instance using a sliding time window of historical and real-time data (the last data point) for prediction.

An AI model can be run in batch mode in which the model is invoked periodically or on-demand, or in streaming mode in which the model run is triggered by the arrival of new real-time data, or

in a hybrid of both modes. In what mode an AI model is run depends on the requirement of the industrial applications that the AI model supports.

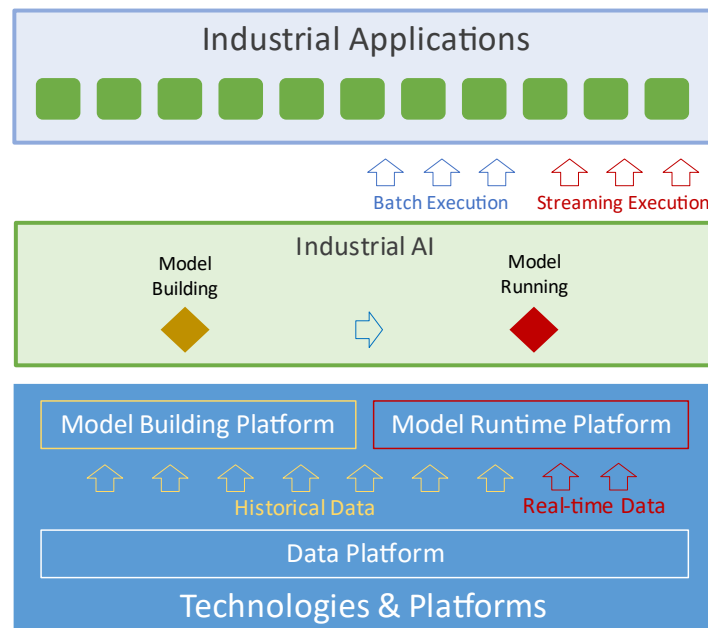


Figure 4-6. Industrial AI High-Level Functional Components.

The general functional architecture for industrial AI described above is generic in the sense that it is applicable whether it is deployed in a remote data center, in local data centers or on the edge. Typically, the model building platform is separate from the model-running platform, but both should share the capability in supporting the same model, with variation in capacities.

It is common that the training of a model requires the processing of large amount of data, whereas the running of model involve smaller amounts of data each time the model is invoked, especially in the streaming mode. In some cases, models may have self-learning capability and can retrain or adjust itself in the run time. In the settings where the output of these type of self-learning models may affect operations of machines or processes, stringent validation and conditions must be implemented to prevent inadvertent outcomes.

It is also common that the model-building platform may require larger amount of processing capacity than the running platform. On the other hand, the runtime platform may require continuous operation, especially in streaming mode, whereas the model building platform is only needed when model building or refinement is in progress.

Access of historical data in the data platform for model building can be on-line (model-building process can access the data platform on-line), or off-line (needed data can be downloaded from the data platform preceding the model building, or even obtained from other sources).

4.5 SYSTEM OF SYSTEMS ISSUES

A system of systems (SoS) is a collection of independent and distributed embedded and physical systems dynamically composed to generate a new and more complex system, provided with new functionality and characteristics, and driven by new goals not present in the constituent systems individually, namely:^{62, 63}

- *Operational independence of the individual systems:* A SoS comprises component systems that are independent and useful, each capable of independently performing useful operations independently of one another.
- *Managerial independence of the systems:* The component systems can operate independently, yet they can achieve an intended purpose.
- *Geographic distribution:* Geographic dispersion of component systems is often large, and often exchange information and knowledge with one another.
- *Emergent behavior:* The SoS can perform functions and carry out purposes that do not reside in any component system.
- *Evolutionary development:* A system of systems is never fully formed or complete. Development of these systems is evolutionary over time, with structure, function and purpose added, removed and modified as the system grows and evolves over time.

Figure 4-7 shows an example of a system of systems in the EV automotive charging space.⁶⁴ Each system is itself a system component in a larger a system of systems. In this example, the AI capabilities may be embedded at various levels of the system-of-systems hierarchy.

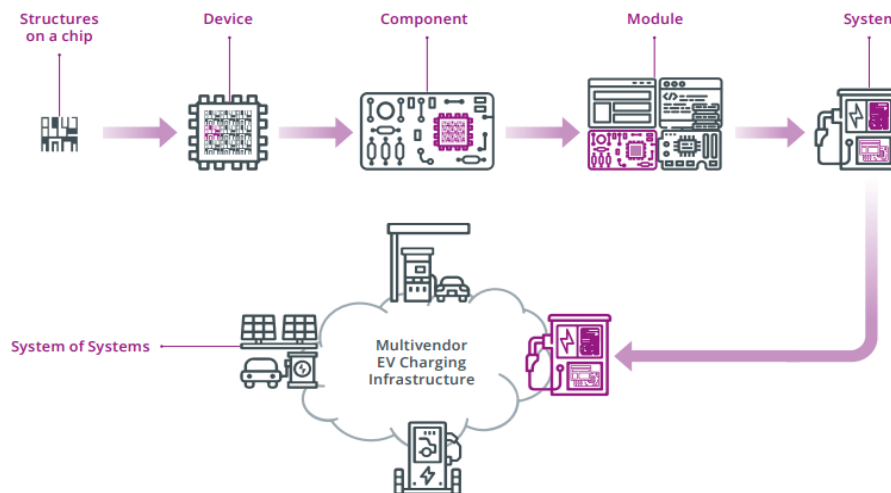


Figure 4-7. Example of a System of Systems in the EV Charging Space. Source: Artemis.

⁶² Artemis: Strategic Research and Innovation Agenda 2021 (Glossary). <https://bit.ly/3iPUOhY>.

⁶³ Department of Systems Engineering, George Mason University: *On the Systems Engineering and Management of Systems of Systems*. <https://bit.ly/37QWmSA>.

⁶⁴ Artemis: Strategic Research and Innovation Agenda 2021 (Figure F1). <https://bit.ly/3iQHw4L>.

The characteristics cited at the beginning of this section must be considered in the various stages of the implementation, namely the requirements definition, the technology selection, and the actual implementation of the AI systems. The design and implementation of the AI systems within a SoS must also take into consideration design and implementation challenges that are typical for SoS, namely architecture (multi-technologies, stakeholders, and evolutionary nature), interoperability between system components, composability of embedded objects and systems engineering of SoS.

4.6 APPLICATION HORIZON OF INDUSTRIAL AI

Industrial AI can be applied in different domains distributed across an IIoT system and tuned to varying time-scale horizons. The required architecture can be analyzed in the context of the functional domains of IIC's Industrial Internet Reference Architecture (IIRA).

An end-to-end IIoT system in the IIRA is functionally decomposed into five functional domains:

- Control: sensing, communication, execution, motion and actuation,
- Operations: provisioning, management, monitoring, diagnostics and optimization,
- Information: data fusion, transforming, persisting, modeling and analyzing,
- Application: logic, rules, integration, human interface and
- Business: enterprise and human resources, customer relationships, assets, service lifecycle, billing and payment, work planning and scheduling.

The control domain is a collection of core functions performed by the industrial assets or control systems. The operations domain is a collection of functions for assets and control systems management and maintenance to ensure their continuing operations. The information domain is a collection of functions for collecting, transforming, analyzing data to acquire high-level intelligence of the entire system.

The application domain is a collection of functions for applying use-case-specific logic, rules and models based on the information obtained from the information domain to achieve system-wide optimization of operations or other business objectives. The business domain is a collection of functions for integrating information across business systems and applications to achieve business objectives.

Industrial AI can be applied to the control domain at the edge, providing real-time operational insights to control loops in a machine-time horizon that requires an analytic response in milliseconds or less. Examples of AI at the edge include autonomous vehicles and smart industrial robotics. Analytics in this time horizon tend to be streaming in nature and applied automatically. Industrial AI can be also applied to the application and operations domains to provide machine insights that enable advanced maintenance processes such as automatic fault-detection and diagnosis, preventive maintenance (e.g. routine equipment checks and repairs) or to drive optimal operations across fleets of machines or assets. The operation-time horizon typically requires an analytic response in the range of seconds or more.

AI in the operation-time horizon also tends to be streaming in nature and is applied automatically. Industrial AI can also be applied to the business domain, providing insights that enable intelligent business processes (e.g. strategic planning) and product design and engineering processes.

The analytics result is applied in a planning-time horizon that typically requires an analytic response in the range of days or more. It consists of both streaming analytics results that are applied automatically in real time (e.g. to work and machine-part scheduling for on-site repair) as well as analytics results that are batch processed based on on-demand queries. Note that the term analytic, as it is used above, encompasses AI machine learning analytics.

5 IMPLEMENTATION VIEWPOINT

The implementation viewpoint (Figure 5-1) deals with the technologies needed to implement functional components (functional viewpoint), their communication schemes and their lifecycle procedures. These elements are coordinated by activities (usage viewpoint) and supportive of the system capabilities (business viewpoint).

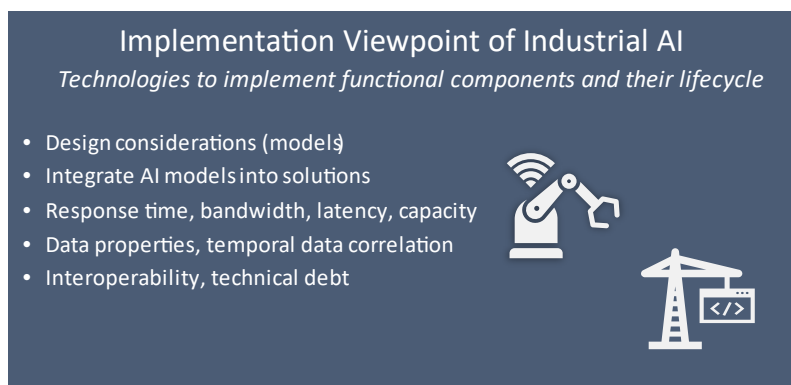


Figure 5-1. Industrial AI Framework Functional Viewpoint and Its Stakeholders. Source: IIC.

The implementation viewpoint relates to considerations around the design and integration of an AI system into an IIoT system. These considerations may be different from those of AI systems in consumer IoT solutions, and encompass model design, system design and the locations and ways within the IIoT system where the AI will be implemented.

5.1 IMPLEMENTATION GUIDANCE

For the implementation of an AI system to be effective, it must address the challenges related to engineering system issues as well as the effect this implementation will have on people. The way an AI system is implemented is unique to the use case and is rarely portable to other use cases, because the requirements specifics and scope of training data sets are always highly dependent on the use case.

On the other hand, the experience of implementing an AI system in a particular use case creates a deep understanding and knowhow about AI technology. This enables management to ask the

right questions and better appreciate the risks involved. This understanding and experience are transferrable across use cases within the organization.

5.2 IMPLEMENTATION CONSIDERATIONS

This section covers the various issues and considerations related to the design and integration of the AI system into the IIoT system.

At a high level, the requirements for implementing AI into applications must be assessed for their suitability, economic viability, and ability to produce solutions that are “industry-ready”:

- Identify the right AI technology for the solution: necessity, suitability, economy.
- Address ethics, bias, explainability and privacy issues.
- Assess the impact of AI-related errors on safety.
- Identify the architectural, integration, and performance requirements of AI.⁶⁵
- Identify the organizational and operational impact of the IT-OT convergence on AI.

The design of the AI system must also meet the performance requirements including data collection, data preparation, AI model learning, and AI model retraining. The stakeholders⁶⁶ must be involved throughout this phase to ensure that their requirements and perspectives are taken into account. Please refer to section 4.3 for more details.

An agile development approach with structured and measured steps across multi-disciplined groups should be employed, facilitating the definition of scope and the integration steps.

5.2.1 SCOPE

The role of AI in IIoT systems is growing in scope and prominence, where the AI system and the IIoT system itself work hand-in-hand across wide range of use cases and deployments.

The scope of the AI should be defined with a high degree of specificity and describe its interactions with the other components of that solution, especially in complex environments that require integrated human-machine interactions and collaboration. For example, in predictive maintenance use cases (in areas like logistics, oil and gas, infrastructure, buildings, aviation and utilities), the trained AI performs predictive analytics on the collected sensor data and identify patterns and anomalies. This insight in turn assists in the determination of the required maintenance tasks and the subsequent scheduling and performance of these tasks.

5.2.2 RESPONSE TIME

A trained AI system that has been integrated within the IIoT system must satisfy specified requirements for response time (operationally), otherwise the performance of the IIoT system may be affected negatively. The response time performance measure may be affected by several

⁶⁵ Refer to sections 4 of this document and the IIC IIRA document.

⁶⁶ Refer to the Usage and Functional Viewpoints: business, technology, data scientists, operations, etc.

key factors, such as where the AI is being performed (within the device, at the edge, in the cloud), and the ability of the integration platform (and its APIs) and consequently the overall IIoT system to achieve and sustain the required data flows and their performance required by the AI system.

Another key factor affecting the response time of an AI system is the performance of underlined hardware over which the AI computation is performed, some AI models may require special hardware acceleration such as GPUs to meet response time requirements. In an IIoT system setting, some processes may require deterministic analysis, computation, and response; others can be done after the fact.

5.2.3 RELIABILITY

Trustworthy AI⁶⁷ is the notion that trust should exist between the user and the system being used and the quality and consistency of the service provided by the AI system when operating within the system. Reliability of AI is part of the notion of trustworthy AI. It is the inherent ability of a trained and tested AI model to perform consistently well.

This issue goes beyond the inherent reliability of the AI system itself. The integration of the AI into the IIoT system must ensure that the reliability of the AI system is not negatively affected. For example, if the AI system does not receive sensor data of sufficient quality and quantity due to reasons such as security breaches or weak bandwidth, it may not perform reliably. That may negatively affect the reliability of the overall IIoT system. Reliability often involves verifications, interpretations, and audits to reveal the inherent robustness of the AI model, before and after it is integrated into the IIoT system.

5.2.4 BANDWIDTH AND LATENCY

The volume of data generated by IoT sensors and control systems can be huge. The design of the network and infrastructure, including the systems and subsystems that incorporate AI, must be optimized, technically and economically, to support these bandwidth and latency requirements.

Increasingly, IIoT systems are incorporating AI-enabled edge computing devices where the AI analytics on the data generated from devices or local networks are processed locally on an edge device itself. Hyperconnectivity technologies like 5G can also significantly affect the bandwidth and latency equation in terms of IIoT system architecture and where AI can be performed. AI-enabled IIoT applications will continue to evolve in scope and diversity. Meeting the growing bandwidth and latency requirements for these applications will continue to be a challenge.

⁶⁷ This is different from AI ethics, which is the ability to distinguish between right and wrong.

5.2.5 CAPACITY

Key properties of the infrastructure include latency, bandwidth, computational and storage capacity, as well as a choice between edge and data center. As an example, it may be desirable, even optimal (for technical or economic reasons) to perform the AI analytics within specific tiers in the IIoT system architecture. If the existing infrastructure cannot support this choice from a capacity requirement point-of-view, a different tier may have to be selected.

5.2.6 SECURITY

Since AI technology is highly dependent on data, the security standards and best practices applied to IT and IIoT systems^{68,69} must be applied to the AI systems that are integrated within them. These security considerations must be addressed throughout the lifecycle of the IIoT system and its integrated AI systems. Refer to section 3.3.1 for details.

5.2.7 DATA PROPERTIES

The data used during AI training, testing and operation is significant in volume and must be dealt with in accordance with best practices that are typically associated with big data, including volume, veracity, and variety, also provenance and integrity.

Volume: The volume of data⁷⁰ generated by the countless sources that an AI system would need to execute its desired functions is massive and growing exponentially. This rapid production of extremely large sets is forcing organizations to gather, store, process and present all of that data in real-time. The storage, compute and bandwidth requirements for such large data volumes must be addressed within the system architecture.

Velocity: With AI, the flow of data is continuous and massive. Below are a few examples:

- IIoT sensor and operational data that are typically produced cyclically.
- High-frequency data, such as vibration or acoustics data from aircraft engines and wind turbines, can significantly increase the speed of data processing needed.
- Transient events where readings must be captured with accurate time recording to determine order of occurrence, causality and root cause.

With these low-latency requirements, AI analytics using high-velocity data is better performed close to where the data is measured. The speed by which all this data can be accessed will be of utmost importance as well, as it will affect the AI system's ability to make decisions. Even a small variation of newly captured data can lead to greater insights and better results. Existing data infrastructures are under real pressure with the increasing volume and velocity of data, coupled with the need to ensure authorized and well-managed access.

⁶⁸ IIC: *Industrial Internet Security Framework*. Refer to Annex C for reference.

⁶⁹ IIC: *Data Protection Best Practices whitepaper*. Refer to Annex C for reference.

⁷⁰ Image data, IR image data, LIDAR data, time series data, text, etc.

Variety: Organizations tend to have a wide range of equipment that have been acquired over the years with dissimilar controls, interfaces and available data. Effective AI analytics depends on shared information models to store, manage, manipulate, understand and analyze this diverse variety of data, in format (syntax) and content (semantics).

Data provenance: The history and sourcing of the data consumed by the AI systems must be captured and recorded for auditing and defensibility⁷¹ purposes. Data provenance is one of the core elements of trustworthy AI. It is metadata that shows where the data came from (including context) and its full system-to-system and custodian-to-custodian “chain of custody”. Related to the above (and part of explainable AI) is the need to track training data, models, algorithms and decision processes to support auditing and accountability determination.

Data integrity: This is a measure of the quality of the data collected and used during AI training, testing and operation. The reliability and integrity of this data must be addressed throughout the lifecycle of both the AI system and the IIoT system.

5.2.8 TEMPORAL DATA CORRELATION

Temporal data correlation is the correlation of data between multiple sensors and process control states, including the crucially important temporal order at which the data is generated and processed. Configuring AI systems closer to where the data is generated reduces the burden of correlation when AI analytics is applied.

5.2.9 INTEROPERABILITY

As the architecture of IIoT systems becomes more distributed,⁷² the AI systems of an IIoT system may interoperate with each other within the context of the overall functionality, namely, to exchange information and to consume and analyze that information.

This interoperability must be supported at multiple levels or layers. The first layer is foundational interoperability, where the data transmitted by one AI system can be received by another. The second layer is structural interoperability, where the format of the received data across multiple systems is standardized. The third layer is semantic interoperability, where the data flowing between two or more AI systems can be interpreted at the receiving end. Standards must be established to define the ways AI systems can receive and process data.

5.2.10 RUNNING SYSTEMS IN PARALLEL

Where possible, organizations should consider running legacy systems and AI-enabled systems in parallel before the latter are deemed to be fully compliant with the design and operational objectives. Such a hybrid approach allows good management of resources, costs, and quality results more efficiently while fine tuning the AI system.

⁷¹ Legal, regulatory, insurance.

⁷² Due to growing use of Edge Computing, 5G and other types of communication technologies.

5.2.11 DEALING WITH TECHNICAL DEBT

Technical debt⁷³ is a metaphor that equates the outstanding cost of poorly factored and poorly written software to financial debt. The debt arises when an organization adopts quick and easy solutions (as opposed to the right ones) during design or implementation, which requires future modifications. Just like financial debt, technical debt comes with the obligation of compound interest, in the form of future re-work and delays.

AI-enabled applications can also suffer from such debt within the design of the AI systems themselves (beyond the scope of this framework) and in the way the models are integrated into the IIoT system. The way an AI system is integrated into an IIoT system may result in technical debt must be mitigated against using traditional strategies and best practices for technical debt mitigation, for example refactoring, comprehensive testing, deleting dead code, reducing dependencies, tightening APIs, and improving documentation.

Paying down technical debt is critical for long-term system health. It also enables algorithmic advances and other cutting-edge improvements.⁷⁴

5.2.12 PORTABILITY AND REUSABILITY OF AI SYSTEMS

For AI to solve real business problems in industry and realize its significant potential, one must adopt a highly focused approach that leverages industry-specific data, domain knowledge and human expertise, such as healthcare, automotive and power.

The ability to reuse and redeploy AI systems into new use cases within the same application domains, whether related or different, presents unique challenges. For instance, training data that would be used in a new use case may have to be entirely new, algorithms may have to be changed and tested, and the AI system itself may have to be enhanced.

The risks associated with AI's lack of accuracy in terms of false positives and false negatives must be assessed, and the implications that this will have on the effectiveness of that application in that specific domain. An algorithm with 90% accuracy may be good enough for predicting incoming customer orders for a particular month. But it will not be suitable for a safety-critical system where wrong predictions may have life-and-death consequences.

Consequently, the cost of reusing and porting an AI system is significantly more than traditional IT systems. Nonetheless, the economies of scale of reusing AI systems within an organization may come from the learning experience of how to integrate an AI system within a business model.

⁷³ Technopedia Ward Cunningham: *Technical Debt*. <https://bit.ly/3xVed5p>.

⁷⁴ *Machine Learning: The High-Interest Credit Card of Technical Debt*. <https://bit.ly/3gaZlcT>.

6 THE FUTURE OF THE INDUSTRIAL AI

The growth and advances of AI over the past decade have been breathtaking and impressive. In this brief period, AI technology has rapidly found its way into a wide range of industries, including healthcare, manufacturing, infrastructure, transportation and many others. This Industrial AI Framework has provided a high-level overview of AI and discussed the issues and concerns related to the application of AI in industry. The document framed these discussions in the context of the four viewpoints as defined in the IIRA: business, usage, functional and implementation.

6.1 FAR-REACHING BENEFITS OF AI DESPITE THE RISKS

Not unlike other technologies, AI is sometimes associated with certain disadvantages and risks. For example, people with malicious intent can train an AI algorithm to cause industrial accidents. If an AI is hacked, the negative consequences can spread through the system with high velocity. AI can also lead to job displacement, for example AI-enabled robots capable of performing simple and repetitive tasks can replace workers on the shop floor.

The disadvantages and risks of AI should not be overstated however, because the use of industrial AI can generate exceptional and far-reaching benefits to society and organizations that far outweigh its disadvantages. The benefits of industrial AI include more precise predictive insights, the ability to perform tasks in hazardous and hard-to-reach spaces, higher work and process efficiencies, to name a few.

Furthermore, despite its job displacement effect, AI can create new and higher paying job categories. It can also act a key enabler of digital transformation empowering organizations to transform themselves radically and the way they deliver value to the marketplace.

AI has already found its way into a wide range of solutions in the industry such as drug and vaccine discovery and manufacturing, disease analysis and diagnosis, radiology, automation of repetitive manufacturing tasks, autonomous vehicles, autonomous robots, asset and process optimization, manufacturing and assembly defect detection and analysis and predictive and preventive maintenance, to name a few.

6.2 CONVERGENCE WITH OTHER TRANSFORMATIVE TECHNOLOGIES

The rapid emergence and convergence of AI with other IT and OT transformative technologies such as IoT, digital twins, edge, XR,⁷⁵ 5G, distributed ledger and other types of technologies, promises to unleash a new generation of highly distributed systems that are personalized, contextualized, and feature real-time human-to-machine (H2M) and machine-to-machine (M2M) interactions, and new human machine interfaces.⁷⁶ This will empower a new generation digital

⁷⁵ Extended Reality.

⁷⁶ Augmented Reality, Virtual Reality, Tactile, etc.

transformational capabilities in organizations in virtually every industrial sector, with AI is acting a main catalyst for such disruptive IIoT solutions.

Edge: AI is often tasked with the processing of significant amounts of sensor data from various platforms in learning, testing and production phases. This places high demand for AI analytics to be performed on edge devices⁷⁷ in close proximity to the physical devices where the data is created.

These demands include the following:

- analyze high volume and velocity data streams at near real-time,
- reduce the costs of data communication between local devices and the cloud because less data will be transmitted and
- process data locally due to privacy and security concerns.

Edge AI is AI performed at the edge close to the physical devices. AI can be deployed in an edge-to-edge configuration where the intelligence is distributed horizontally, such as V2X⁷⁸ and smart factory, or in an edge-to-cloud configuration where the intelligence is distributed vertically between the edge and the cloud, such as image recognition and smart building.

As available computing power continues to grow, researchers have recently surveyed⁷⁹ different ways AI can be deployed using edge computing technology. Driven by visions of IoT and 5G communications, edge computing systems are capable of integrating computing, storage, and network resources at the edge of the network to provide local computing infrastructure, enabling developers to quickly develop and deploy applications.

Hyper-connectivity: Given the distributed nature of IIoT systems, the raw data is typically produced in geographical and architectural areas that are separate from where they are used. This means that the networking and connectivity aspects of IIoT systems are critical to the overall design and operation of these solutions. Furthermore, requirements for intelligent operation “beyond visual line of sight”⁸⁰ are placing high demands on systems in terms of more autonomy and agility, lower latency and more precision.

5G⁸¹ is a hyper connectivity technology that enables ultra-reliable low-latency communications (URLLC), enhanced mobile broadband (EMB) and massive machine type communications (mMTC). This enables highly distributed IIoT applications⁸² through dramatic improvements⁸³

⁷⁷ IIC: *Introduction to Edge Computing in IIoT*. Refer to Annex C for details.

⁷⁸ Vehicle to X: infrastructure, other vehicles, etc.

⁷⁹ F. Liu, G. Tang, Y. Li, Z. Cai, X. Zhang and T. Zhou, "A Survey on Edge Computing Systems and Tools," in *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1537-1562, Aug. 2019. <https://bit.ly/3spmjSC>.

⁸⁰ Autonomous inspection drones, autonomous vehicles, remote surgery, etc.

⁸¹ IIC: *Industrial Networking Enabling IIoT Communication*. <https://bit.ly/3poye26>.

⁸² Wide range of sectors, including logistics, transport, manufacturing, energy, healthcare, and utilities.

⁸³ Much higher upload and download broadband speeds, ultra-reliability, very low-latency, support for network slicing and support for high-density machine-to-machine communication.

over previous generations of wireless broadband technologies. With the combination of 5G and edge, AI can be distributed deeper into the different segments of the architecture, raising the importance of addressing the viewpoint concerns described earlier in this framework.

Digital twin: Digital twins are dynamic digital replicas of physical entities that help organizations make model-driven decisions. The benefits of digital twins include lower maintenance costs via predictive maintenance, improved productivity and testing prior to manufacturing, leading to better business outcomes and higher customer satisfaction.

AI and digital twins contribute to each other. Digital twins can help organizations generate simulated data which can be used to train and test AI models and to deploy AI-enabled IIoT solutions. On the other hand, AI enables businesses to build more effective digital twins and process the vast amounts of data collected from these digital twins. For example, engineers can accelerate design processes and improve how product design changes are managed.

Brain-computer interface: Brain-computer interface (BCI) is a cross-disciplinary research domain that aims at leveraging advancements in neuroscience and AI to promote the ability of the human brain to communicate and interact with the environment. The combination of BCI and AI technologies promise to lead to the development of innovative thought-powered communication and robotic solutions for people with disabilities and knowledge workers in highly demanding tasks.

Quantum computing: Despite the rapid progress that AI has made over the past decade, it has yet to overcome major technological limitations such as the rapid training of complex machine learning models to create optimized algorithms. Neuromorphic cognitive models, adaptive machine learning, or reasoning under uncertainty are challenging for today's AI. Quantum AI is the use of quantum computing for computation of machine learning algorithms. By leveraging the computational advantages of quantum computing, quantum AI can help achieve results that would not be possible with classical computers. Quantum AI promises to overcome these challenges and complete years of analysis in a short time and lead to advances in technology.⁸⁴

6.3 STANDARDS ECOSYSTEM

The work done by the ISO/IEC JTC 1/SC 42 (Artificial Intelligence) is a prime example of the emerging ecosystem for AI standards. SC 42 is a joint committee of the International Organization for Standardization (ISO)⁸⁵ and the International Electrotechnical Commission (IEC).⁸⁶ SC 42 serves as the focus and proponent for JTC 1's⁸⁷ standardization program on Artificial Intelligence

⁸⁴ <https://research.aimultiple.com/quantum-ai/>

⁸⁵ <https://www.iso.org/home.html>

⁸⁶ <https://www.iec.ch/homepage>

⁸⁷ JTC 1 is the standards development environment where experts come together to develop worldwide Information and Communication Technology (ICT) standards for business and consumer applications. <https://www.iso.org/committee/45020.html>

and provides guidance to JTC 1, IEC and ISO committees developing Artificial Intelligence applications.⁸⁸

This section summarizes and builds upon a paper⁸⁹ written by Wael William Diab, the Chair of this committee, and titled “Enabling the digital transformation of industry: The roles of AI, big data, analytics, and related data ecosystem”.

The committee is developing international standards for AI with the goal of accelerating AI adoption while simultaneously addressing emerging issues to enable successful digitalization of sectors such as smart manufacturing.

6.3.1 ENABLING INTELLIGENT INSIGHTS

Many of the emerging services rely on the ability to provide insights based on the large amount of data being generated, such as operational real-time data and batch data. The technologies on which SC 42 is working will facilitate such services, for example:

- AI technologies will allow insights and analytics that go far beyond what legacy analytic systems could provide in terms of efficiency, speed, and applications that have yet to be envisioned. This is a radical departure from the way in which analytic systems have traditionally been designed akin to the “plug-and-play” approach in enterprise and consumer applications more than a decade ago.
- Big data technologies will streamline and, in many cases, enable analytics to be performed on massive data sets. This will be achieved by designing computer system architecture around how the data sets will be generated and used in a particular application, rather than applying the same computer system to an application regardless of what the data looks like in terms of its variety, volume, variability, and so on.

SC 42 is considering some of the concerns about the usage and application of these technologies. Data quality standards for machine learning and analytics are crucial for helping ensure the applied technologies produce useful insights and eliminate faulty features. Governance standards in AI and the business process framework for big data analytics address how the technologies can be governed and overseen from a management perspective. Standards about trustworthiness, ethics, and societal concerns from the outset will help ensure rapid and effective deployment.

SC 42 is also working on a novel approach to instill confidence when technologies such as AI are used through a management system standard.

⁸⁸ <https://www.iso.org/committee/6794475.html>

⁸⁹ <https://www.raps.org/news-and-articles/news-articles/2021/6/enabling-the-digital-transformation-of-industry-th>

6.3.2 ECOSYSTEM APPROACH

SC 42 is taking an ecosystem approach by looking at emerging requirements from a variety of stakeholders such as business, domain specific, regulatory, societal and ethical requirements. The committee assimilates these requirements, translates them into technical requirements and develops horizontal deliverables that are applicable across industries.

This platform approach enables SC 42 to collaborate with other organizations and committees and provide a framework for application domains, such as smart manufacturing, to build upon and use the work of SC 42. The diagram below summarizes the approach.

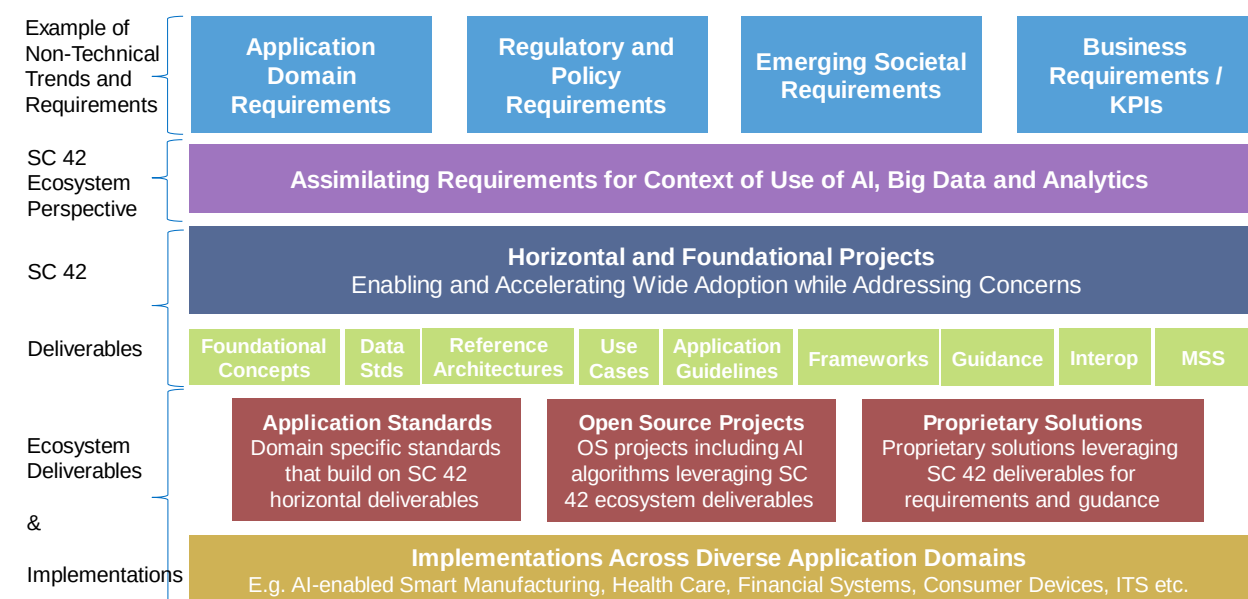


Figure 6-1. Trustworthiness of IIoT Systems. Source: ISO /IEC JTC 1/SC42.

6.3.3 PROGRAM OF WORK AND ROLE IN ENABLING DX ACROSS INDUSTRIES

The exemplary list below shows the role of the SC 42 International Standards in enabling digital transformation in industry sectors such as smart manufacturing:

Application guidance and use cases: SC 42 collects use cases to ensure that its horizontal standards are broadly applicable and provide guidance to AI application domain developers and application domain standards groups. SC 42 is also developing guidelines for AI applications that enables application developers, open-source communities and application SDOs/committees to leverage the work of SC 42. In addition, a standard on AI system life cycle processes is being developed.

Foundational standards: With technologies like AI expected to become ubiquitous in the near future, the diversity and number of stakeholders will continue to increase. Foundational standards provide a common language and frameworks that can be used in this regard.

Trustworthiness: Due to its wide applicability, trustworthiness aspects of AI are critical and necessary for broad adoption. SC 42 has published a suite of standards that provide an overview of these emerging issues such as trustworthiness, robustness, and bias. In addition it is developing technical standards to address these aspects that include: the application of the ISO 31000 risk management framework to AI, quality model for AI systems, quality evaluation guidelines, explainability, controllability, transparency taxonomy, assessment of neural networks and treatment of unwanted bias.

Ethical aspects and societal considerations: New requirements around ethics and societal concerns have emerged with recent information technologies, and AI is no exception. SC 42 is addressing these concerns across the board in its deliverables – for example, ethical and societal concerns around use cases – as well as specifically, by having deliverables that tie these requirements to the technical standards being developed.

Data ecosystem: SC 42 is addressing the AI data ecosystem and has launched a five-part series on data quality for machine learning and analytics. In addition, SC 42 is developing a new AI data lifecycle framework. These efforts complement the data ecosystem work in progress on big data analytics as well as the published foundational standards on big data.

Governance implications: SC 42 is collaborating with SC 40 to develop a standard targeted at addressing governance implications that can arise. The standard under development is aimed at and tailored for executives or boards looking to deploy AI technology.

Computational aspects: At the heart of AI systems are the computational technologies. SC 42 is looking at the computational approaches and characteristics of AI systems. It has published an overview of the state of the art of computational approaches for AI systems which describes the main computational characteristics, algorithms and approaches used in AI systems, referencing use cases. SC 42 is working on projects in this area that range from a reference architecture for knowledge engineering, which is focused on the front end of the process, to the assessment of classification performance for machine learning models.

Management systems standard: The unique aspects of AI technology have created a need for a methodology that covers developers and deployers of AI systems. This will help increase user confidence by providing a platform that can be used for third-party certification. SC 42 is leveraging the management systems standard (MSS)⁹⁰ approach and has started work on ISO/IEC 42001 for an AI management system.

⁹⁰ MSSs have been successful in other areas, such as ISO 9001 and ISO/IEC 27001

6.3.4 SUMMARY

As with the smart manufacturing inflection point, the core value of digital transformation is the ability to provide insights. Technologies such as AI, analytics and big data are enablers for this transformation. The international standards that SC 42 is developing will remove barriers to adoption while addressing concerns. Nonetheless, these standards and technologies will have to be used in concert with operational technology standards, such as those being developed by ISO and IEC committees.

SC 42's unique approach to consider the entire ecosystem and develop horizontal standards allows for a platform that makes such collaboration easier than vertical application standards can build upon. The platform facilitates the goal of broad responsible adoption of AI by enabling a diverse variety of stakeholders to build on its work. These include SDOs/standards committees looking at applications, AI developers and technologists, business, industry, regulatory, social scientists, opens source communities and society at large.

6.4 FINAL THOUGHTS AND TAKEAWAYS

Today, AI is embedded in a wide range of applications, helping organizations in industry achieve the sought-after benefits and transform how they operate and deliver value to the market.

We should expect the adoption of AI to continue and accelerate in the industry:

AI technology: The increase of compute power, the wider availability of training data sets, and the growing sophistication of algorithms will lead to more intelligent AI capable of performing more and more challenging tasks.

Apply current standards and best practices to AI: Organizations should consider adopting a top-down and risk-based approach to dealing with AI in the enterprise. Established principles, industry standards, and best practices for business, IT, security, operations and compliance must be applied to AI-enabled systems. At the same time, considerations related to AI's unique characteristics must be addressed throughout lifecycle of the AI-enabled IIoT systems. The comprehensive platform of standards looking at the entire AI ecosystem being developed by ISO/IEC JTC 1/SC 42 (Artificial intelligence) are a good example.

AI for IoT is more than AI for IT: The physical-digital nature of IIoT systems introduces specific considerations related to safety, reliability and resilience concerns, among other things. These concerns must be addressed within the design of the AI system and the way it is implemented and used within the IIoT system.

Maturity about AI: The growing maturity of organizations about AI and its uses, will help them appreciate the reality that the benefits of AI far outweigh its risks. Organizations must however persist in their risk assessment efforts about using AI and mitigate against these risks.

AI will continue to push the technological state-of-the-art of what is possible. Attitudes towards the technology and business expectations about its use will also continue to evolve. Thus *what is considered to be the reasonable thing to do* will also evolve.

The issues and guidance provided in this document were framed with this evolution in mind. In the future, we can expect the use of AI technologies to become the norm rather than the exception. Given the societal benefits of using AI, “not using AI” may eventually become *the irresponsible thing to do*.

Annex A ARTIFICIAL INTELLIGENCE BACKGROUND

AI is not new. People have always wondered whether computers can perform intelligent tasks, especially tasks that are easy for humans but are hard to code formally.

A.1 BRIEF HISTORY OF AI

In the 1950s, Alan Turing, the British computer scientist, authored a paper that hypothesized that one day it will be possible to create machines that can think. Turing also created the “Turing test” to establish a definition of “thinking”. In 1956, Professor John McCarthy of Dartmouth University (NH) coined the term Artificial Intelligence (AI) in a study that took the premise that all aspects of learning and intelligence can be prescribed in machines that can simulate it.

Since those early days of computing, AI has gone through several iterations and generations. In the early 2000s, efforts by scientists in artificial neural networks (ANNs), a sub-discipline of machine learning, more specifically in deep learning (DL), notably Professors Geoffrey Hinton (University of Toronto), Yann LeCun (New York University), and Yoshua Bengio (Université de Montréal), led to rapid improvements in AI engine capabilities, accuracy and speed.

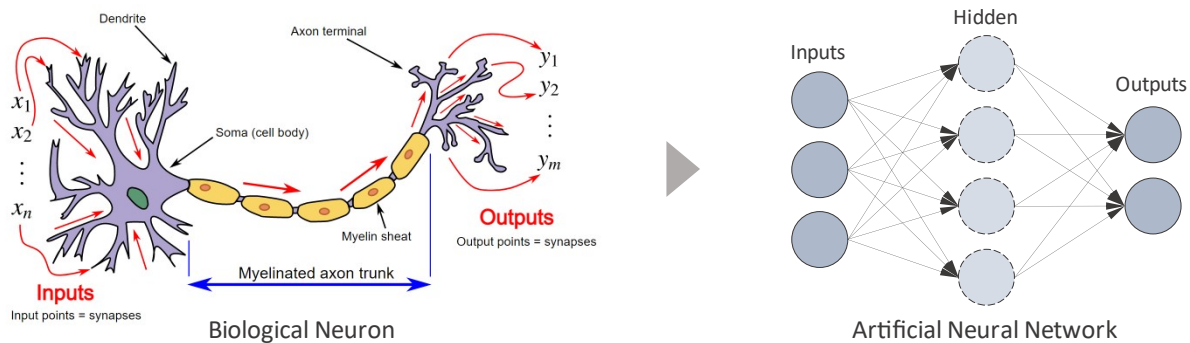


Figure A-1. Biological Neurons and Artificial Neural Networks. Source: Wikipedia.

The development of AI has focused on mimicking how the human brain processes the information captured by the main senses: image recognition, natural language processing (NLP), pattern recognition, and decision making. AI can achieve this at a scale and depth of detail that are impossible for humans to replicate. ML-based AI includes supervised learning, unsupervised learning, semi-supervised learning, and reinforcement learning.

Machine learning and related AI technologies are gaining attention because of their usefulness in the design, manufacture, operation, management and improvement of modern industrial assets. ML algorithms help provide improved product designs and more intelligent asset management. In typical applications, assets with adaptive or learning algorithms continuously learn or adapt their operation based on real or virtual data streams to improve operational stability and efficiency in dynamic environments.

AI comprises many fields such as knowledge graph and expert systems, and not all of them are growing at the same rate. The highest growth is in machine learning, specifically deep learning.

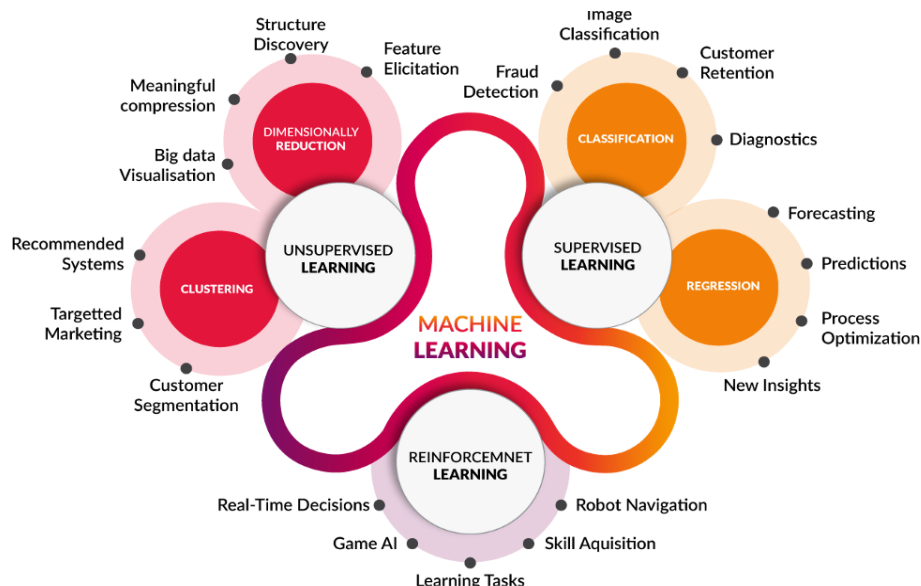


Figure A-2. Types of Machine Learning. Source: COGNUB.

A.2 WHY NOW?

What sparked this latest and sudden wave of AI is the convergence of three key enabling factors: the availability of cheap compute power, big data that can be used for model training and testing, and significant improvements in algorithms.

A.2.1 CHEAP AND POWERFUL COMPUTE INFRASTRUCTURE

Throughout its history, the success of applying neural networks—the core concept behind deep learning—is highly dependent on computing power. While the concept was introduced in 1940s and enjoyed tremendous growth and hype throughout 1950s and 1960s, it effectively died down due to the level of computing power at the time that restricted neural networks from having more than one hidden layer—significantly limited its ability to recognize more complex patterns.

It was not until 1980s, that researchers were able to implement neural networks with more than one layer effectively, removing many of the limitations in the late 1960s, ushering the second coming of neural networks.

Today, with the support of GPUs and specialized hardware like TensorFlow⁹¹ processing unit (TPU), modern neural networks could have thousands hidden layers, millions of neurons with much more complex organization-wise. Alpha Go Lee—the Alpha Go used to beat 9-dan professional Go Player, Lee Sedol, in March 2016—uses 48 TPUs, 1,202 CPUs and 176 GPUs.

⁹¹ An end-to-end open-source machine learning platform. <https://www.tensorflow.org/>.

One short year later, AlphaGo Zero—powered simply by 4 TPUs, 64 GPUs, 19 CPUs—was able to beat the Alpha Go Lee 100. These significant improvements in computing power allow for this equally significant leapfrogging.

A.2.2 AVAILABILITY OF LARGE AMOUNTS OF DATA

Every minute, 55k Instagram photos are posted, 300 new Facebook profiles created, 511k messages tweeted, and 188 million emails sent. According to one estimate, 2.5 exabytes (2.5 million terabytes) are created every day. This trend will continue to accelerate, especially when we factor in the growth in mobile and real-time data (namely data generated by IIoT and autonomous objects). An Airbus A350—equipped with roughly 6k sensors—generates 2.5 TBs per day. Today's autonomous vehicles generate 4 ~ 6 TBs per day. IDC has estimated that the amount of data subject to analysis will grow to 5.2 zettabytes (5.2 billion TBs) in 2025. Simultaneously, storage costs (per unit) will continue to go down.

For ML to work, it needs to be trained with relevant data. In general, the more data it is fed, the more robust the algorithm is. With the rise of the internet, online and mobile services and IoT, there is no shortage of data on which to train ML.

A.2.3 IMPROVEMENTS IN ALGORITHMS

Cheap and powerful compute infrastructure along with plentiful data provide a fertile ground for researchers to run experiments to refine existing algorithms as well as design new ones. Over the past decade, the field of ML specifically deep learning—has flourished with better and faster algorithms from backpropagation, stochastic gradient learning, convolutional neural network and federated learning to generative adversarial networks.

This new generation of algorithms is much more accurate and robust than its predecessors and provides faster outcomes. This allows AI to permeate many parts of our lives. In businesses, AI algorithms are assisting in forecasting, decision making and process automation. AI is also making significant inroads in the areas that are traditionally not its strength, due to its traditional reliance on human nature driven by emotions, such as designing products, composing music, and producing auction-worthy artwork.

Annex B EXEMPLARY USE CASES OF AI IN INDUSTRY

AI technology is key for unlocking the potential of IIoT and enabling digital transformation. AI may also be implemented within an IIoT system in conjunction with other technologies that are also disruptive, for example digital twins, hyperconnectivity (including 5G), distributed ledger, human machine interfaces (AR, VR, etc.) and many others.

The figure below shows exemplary use cases of AI in various industry verticals.

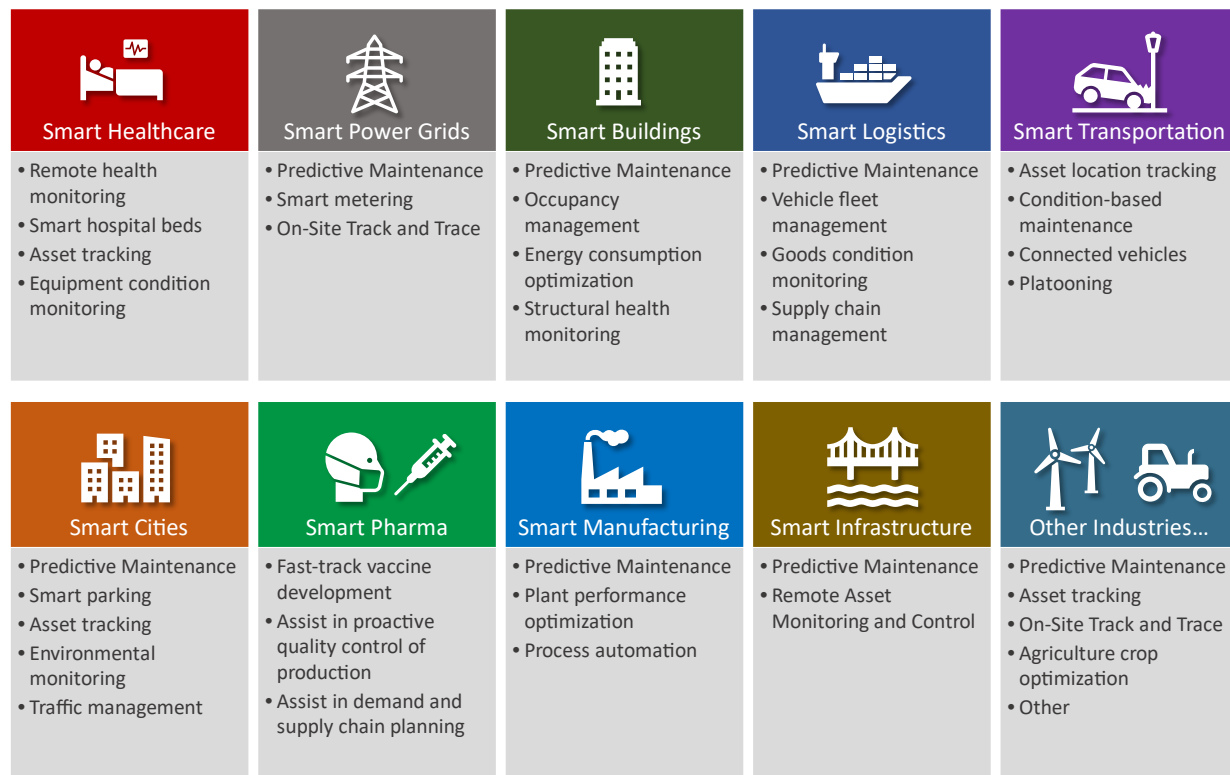


Figure B-1. Exemplary Use Cases of AI in Industry Verticals. Source: IIC.

B.1 MANUFACTURING

Predictive maintenance is a common application of AI technology in a wide range of industries, including manufacturing. AI-enabled sensors can be used to help predict when a piece of manufacturing equipment will be due for a quality check before it breaks down. This allows maintenance work to be scheduled during planned downtime without affecting production.

Prior to the application of AI, factory managers engaged in time and resource-intensive processes with the aim of deciding when to invest resources in routine asset maintenance and repair. Information was painstakingly collected, collated and analyzed using manual processes with the aim of informing decision making around quality assurance tasks.

In AI-enabled scenarios, connected devices can automatically gather real-time intelligence around equipment conditions, analyze this data for trends, run this data through sophisticated algorithms to draw insights and accurately assess when asset maintenance activities are needed to reduce costly unplanned equipment shutdowns. Continuous improvement can be embedded in maintenance plans through the incorporation of ML capabilities that enable “lessons learned” and self-correction mechanisms.⁹²

⁹² IoT Analytics: *The Top Industrial AI use cases*. <https://bit.ly/3CWbqMQ>.

The table below illustrates a use case for AI technology in the steel manufacturing space.

Use Case: Steel Grade Manufacturing Service	
<u>Industry Sector:</u> Manufacturing	<u>Industry Vertical:</u> Steel Manufacturing Industry
<u>Use Case Description</u> The QA Departments of steel manufacturers need to test samples of the steel they produce to make sure it meets steel industry standards (ASTM E-45, JIS G-055). To address that market need, Toshiba sold steel manufacturers a steel inspection equipment, called MetalSpector, that comprised an auto-focus optical microscope, X-Y stage, color area sensor camera, and an image processor. Using the MetalSpector system has multiple challenges: • labor intensive QA process, • long inspection hours caused by increasing number of samples, • lack of consistency in grading judgement depending on inspector, • skill transfer difficulties from veteran inspectors to junior inspectors and • product quality data fraud. In 2020, Toshiba introduced a new AI-enabled <i>Steel Grade Evaluation Service</i> (“as-a-service”) to replace MetalSpector. This offering was designed to reduce the steel inspector workload while assuring steel quality data integrity. The steel inspection process was changed to an IIoT service that connects the microscope image to a data management system and data-center-based AI steel inspection model. The system operates as follows: • capture steel images using a digital microscope and then transfer and store the images to a historian database, • transfer image data with a batch sequence number to the data center for feeding an AI model estimator, • store steel grade result estimated by AI model with sequence number to the log database and • inspectors determine final quality decision by referring to the estimated steel grade.	
<pre> graph LR subgraph "Steel Grade Evaluation Service" SGES((Steel Grade Evaluation Service)) LD[(Log Data)] DM((Data Management)) IDH[(Image Data Historian)] SGES <--> LD SGES <--> DM LD <--> DM IDH --> DM end subgraph "Cloud Computing" AIModel[AI Model] WEBAPI[WEB API] CC[Cloud Computing] WEBAPI <--> AIModel end IDH -- "Image Data" --> DM DM -- "SeqNo+Data" --> WEBAPI AIModel -- "SeqNo+Result(Grade)" --> LD LD -- "Estimated Steel Grade" --> Inspector[Inspector] </pre>	

Use Case: Steel Grade Manufacturing Service

Business Value

Company Transformation:

- Business application mindset changed from product function to product usage.
- Business revenue stream has been gradually changed from a hardware sales model to an as-a-service sales model.

Customer Transformation:

- Data integrity is assured by storing in a secure database which eliminates data fraud.
- Once the AI model training is complete, it is used for not just inspection, but also used for junior inspector education which enables improved transfer of skills to the next generation.

AI Application in Use

- The AI system is integrated within the solution offering.
- It receives digital images of steel along with client identifier and batch sequence number.
- AI model analyzes the digital images and estimates the steel grade.
- Steel grade estimate is sent back to the client through the service offering where it is used to assist their QA inspectors in making the final decision about the steel grade quality.

B.2 HEALTHCARE

AI's ability to bring together vast amounts of healthcare data is steadily transforming the healthcare industry and is bringing new opportunities –and risks–to the management of human health. Below is a sampling of applications of AI in the healthcare industry:⁹³

- medical diagnostics with image analysis,
- validate the need for surgery with predictive analytics,
- diagnose infectious disease with machine learning,
- early detection of dementia with AI,
- virtual health assistants,
- robotic surgery,
- AI in drug discovery and production,
- converting doctors' unstructured notes with NLP,
- track scattered mobile equipment throughout the hospital using AI,
- predict the needs of hospital equipment, supplies and pharmacy,
- predictive maintenance for medical equipment,
- streamline patient registration and onboarding processes with AI and RPA,⁹⁴
- personalize treatment plans using AI-powered analysis of patient's medical history and
- medical records extraction and automation.

AI is also driving the modern hospital and becoming a key enabler of clinical trials.⁹⁵

⁹³ Analytics Insights: <https://bit.ly/3FjSkku>.

⁹⁴ Robotic Process Automation.

⁹⁵ Pharmaceutical Technology. <https://www.pharmaceutical-technology.com/features/ai-in-healthcare-2021/>.

For example, AI-enabled patient diagnostics can enable remote, real-time monitoring of patient health information via wearable devices, where alarms could be automatically triggered to notify care providers as soon as a patient's metrics vary too much from healthy baseline values.

With the help of AI, the medical condition of patients can also be assessed against databases of "like-patient" populations to predict the most statistically viable treatment or medication for a unique patient's specific condition. This leads to quicker and better care decisions resulting in better health outcomes.

B.3 BUILDINGS

Energy cost reductions provide better return on investment for buildings. Energy-efficient buildings are designed to achieve a balance between energy demand and supply to reduce energy consumption. IIoT enables realizing energy efficiency in building infrastructure.

However, building installations are complex and may span several acres. This requires a wide variety and a substantial number of sensors across the facility that sense ambient conditions, sun exposure, traffic flow and occupancy. In addition to people, buildings comprise assets that consume energy, such as HVACs, fans, lights and elevators.

Machine learning can be used to train neural network models for each piece of equipment. Models are tailored to each piece of equipment characteristics. Unsupervised learning can allow equipment and operating anomalies to be detected and identified without labeled training data.

By applying AI-based analytics to IIoT sensor data generated by the building systems, it is possible to generate actionable insights that improve energy consumption efficiency. For example, based on the historical occupancy data, the building can optimize the flow of hot/cold air from the HVAC system to the appropriate sections of the building (rather than the entire building). Energy intensity measurements can also be used to measure the amount of improvement, in support of the energy and corporate sustainability initiatives.

Other AI-enabled "smart building" solutions include:

- Assess the structural condition of a building using solutions powered by AI, drones and digital twins. Such facilities-inspection solutions can produce insights about the structural condition of buildings (and the progression of that condition) with a high level of accuracy and fidelity.
- Detect improper equipment function. Individual equipment and assets are monitored for proper function across a variety of operating scenarios. Equipment not functioning correctly is detected and alerted for maintenance.
- Improve control program settings. Modeling of energy usage across operating conditions is used to identify changes to control program settings for improved efficiency.
- Predict impending equipment failure. System monitoring will detect performance degradation and approaching failure of equipment. Maintenance can be scheduled prior to failure to avoid unplanned downtime.

B.4 TRANSPORTATION AND LOGISTICS

The application of industrial AI in transportation and logistics generates a wide range of benefits and added value, for example:

Demand forecasting: With the help of AI, organizations can better predict demand trends, speed up delivery, implement dynamic pricing and improve and further personalize customer service.

Warehouse automation and management: AI and robotics can perform warehouse tasks with greater speed and precision. This can reduce errors and free personnel from repetitive tasks, example merchandise handling during order fulfillment, better quality and damage control using AI vision.

Supply chain planning and management: AI and IoT can help organizations instrument and interconnect their supply chains and make them more intelligent. With AI, organizations can get a bird's-eye view of the supply chain operation and provide tips about optimizing it and making it more cost efficient, example route optimization and peak hour predictions. AI can also be leveraged in the security of the supply chain (detecting cyber threats, physical theft).

Autonomous vehicles: cars (safer, more fuel efficient, etc.), trucks, platoon driving, carriers, autonomous ride sharing, ships and drones.

Naturally, the above features and benefits are not due to AI alone. However, AI is a major contributor to these benefits and value add.

B.5 DETECTING IIOT SYSTEM THREATS USING AI

A growing application usage of AI technology in IIoT is threat detection, specifically to use AI to augment the security of IIoT systems, including systems that are not AI-enabled.

The proliferation of IoT devices in enterprises has precipitously expanded the attack surface for IIoT systems. While operators of such systems have well-established OT-centric processes to address the security and software upgrades for these machines, standard information technology security practices developed for business systems cannot be applied “as is” to the security of IIoT systems.

The main reason is that these best practices do not cater for the requirements and best practices for safety, reliability and resiliency of physical machines and in some cases may conflict or even contradict with them.

Implementing a security strategy for IIoT systems is challenging because attack surfaces can span the IT/OT divide. These challenges are technological, organizational and procedural. AI technology can improve the ability of the organization to detect threats across that divide more precisely and more accurately, manage vulnerability more efficiently and reduce security-related human errors.

AI technology can be leveraged to augment the security defenses of IIoT systems:

- rapidly and efficiently analyzing billions of IoT sensor-generated data signals that flow through the network infrastructure,
- manage vulnerabilities more efficiently,
- detect security threats and malicious activities in real-time and predict them,
- reduce security-related human errors and
- generate autonomous responses.

Annex C IIC REFERENCES

IIC references	Details and URLs
Data Protection Best Practices	IIC Data Protection Best Practices, v1.0, released July 2019 https://www.iiconsortium.org/pdf/Data_Protection_Best_Practices_Whitepaper_2019-07-22.pdf
DX In Industry	Digital Transformation in Industry Whitepaper, v1.0, released July 2020 https://www.iiconsortium.org/pdf/Digital_Transformation_in_Industry_Whitepaper_2020-07-23.pdf
Edge Computing	Introduction to Edge Computing in IIoT https://www.iiconsortium.org/pdf/Introduction_to_Edge_Computing_in_IIoT_2018-06-18.pdf
IIAF	Industrial Internet Analytics Framework, v1.0, released February 2017 https://www.iiconsortium.org/industrial-analytics.htm
IIRA	Industrial Internet Reference Architecture, v1.9, released June 2019 https://www.iiconsortium.org/IIRA.htm
IISF	Industrial Internet Security Framework, v1.0, released September 2016 https://www.iiconsortium.org/IISF.htm
IITFF	The Industrial Internet Trustworthiness Framework Foundation, v1.0, released July 2021 https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf
Jol Jun 2019 – Article 6	IIC – Journal of Innovation June 2019 issue - Accelerating Performance with the Artificial Intelligence of Things – Jane Howell, SAS https://www.iiconsortium.org/news/joi-articles/2019-June-Jol-Accelerating-Performance-with-the-Artificial-Intelligence-of-Things.pdf
Jol Nov 2019 – Article 6	IIC – Journal of Innovation November 2019 issue - Artificial and Human Intelligence with Digital Twins – Michael Thomas, SAS; Brad Klenz, SAS; Prairie Rose Goodwin, SAS https://www.iiconsortium.org/news/joi-articles/2019-June-Jol-Accelerating-Performance-with-the-Artificial-Intelligence-of-Things.pdf

IIC references	Details and URLs
JoI Nov 2021 – Article 3	IIC Journal of Innovation Article: The Digital Transformation Journey in the Enterprise and its Leadership—Bassam Zarkout, IGnPower https://www.iiconsortium.org/news/joi-articles/2021-November-JOI-The-Digital-Transformation-Journey-in-the-Enterprise-and-its-Leadership.pdf
Industrial Internet Vocabulary	Industrial Internet Vocabulary Technical Report, version 2.3, September 2020 http://www.iiconsortium.org/vocab/index.htm

Annex D AUTHORS & LEGAL NOTICE

Copyright © 2022, Industry IoT Consortium®, a program of Object Management Group, Inc. (“OMG®”). All other trademarks in this document are the properties of their respective owners.

All copying, distribution and use are subject to the limited License, Permission, Disclaimer and other terms stated in the Industry IoT Consortium Use of Information – Terms, Conditions & Notices, as posted at <https://www.iiconsortium.org/legal/index.htm> - use_info. If you do not accept these Terms, you are not permitted to use the document.

This document is a work product of the Industry IoT Consortium Industrial Artificial Intelligence Task Group, chaired by Wael William Diab⁹⁶.

Editorial Team: Bassam Zarkout (Chief Editor) and Wael William Diab (Editor).

Authors: The following persons contributed substantial written content to this document: Wael William Diab, Alex Ferraro (PwC), Brad Klensz (SAS), Shi-Wan Lin (Thingswise), Edy Liongosari (Accenture), Wadih Elie Tannous (AASA), Bassam Zarkout (IGnPower).

Contributors: The following persons contributed valuable ideas and feedback that significantly improved the content and quality of this document: Eric Harper (ABB), Salim Abi-Azzi (Dell).

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

⁹⁶ Section 6.3 and related material are contributed by Mr. Diab as Chair of ISO/IEC JTC 1/SC 42. Other contributions are with his Futurewei affiliation.