SCSA1701 CYBER PHYSICAL SYSTEMS

UNIT 1- INTRODUCTION TO INDUSTRY 4.0 AND CYBER PHYSICAL SYSTEM

A **cyber-physical system** (**CPS**) or intelligent system is a computer system in which a mechanism is controlled or monitored by computer-based algorithms. In cyber-physical systems, physical and software components are deeply intertwined, able to operate on different spatial and temporal scales, exhibit multiple and distinct behavioral modalities, and interact with each other in ways that change with context.CPS involves transdisciplinary approaches, merging theory of cybernetics, mechatronics, design and process science. The process control is often referred to as embedded systems. In embedded systems, the emphasis tends to be more on the computational elements, and less on an intense link between the computational and physical elements. CPS is also similar to the Internet of Things (IoT), sharing the same basic architecture; nevertheless, CPS presents a higher combination and coordination between physical and computational elements.

Examples of CPS include smart grid, autonomous automobile systems, medical monitoring, industrial control systems, robotics systems, and automatic pilot avionics.Precursors of cyber-physical systems can be found in areas as diverse as aerospace, automotive, chemical processes, civil infrastructure, energy, healthcare, manufacturing, transportation, entertainment, and consumer appliances.

1.1 INDUSTRY 4.0

Industry 4.0 refers to the fourth industrial revolution, although it is concerned with areas that are not usually classified as industry applications in their own right, such as smart cities

Fourth Industrial Revolution

The first industrial revolution came with the advent of mechanisation, steam power and water power.This was followed by the second industrial revolution, which revolved around mass production and assembly lines using electricity.The third industrial revolution came with electronics, I.T. systems and automation, which led to the fourth industrial revolution that is associated with cyber physical systems.

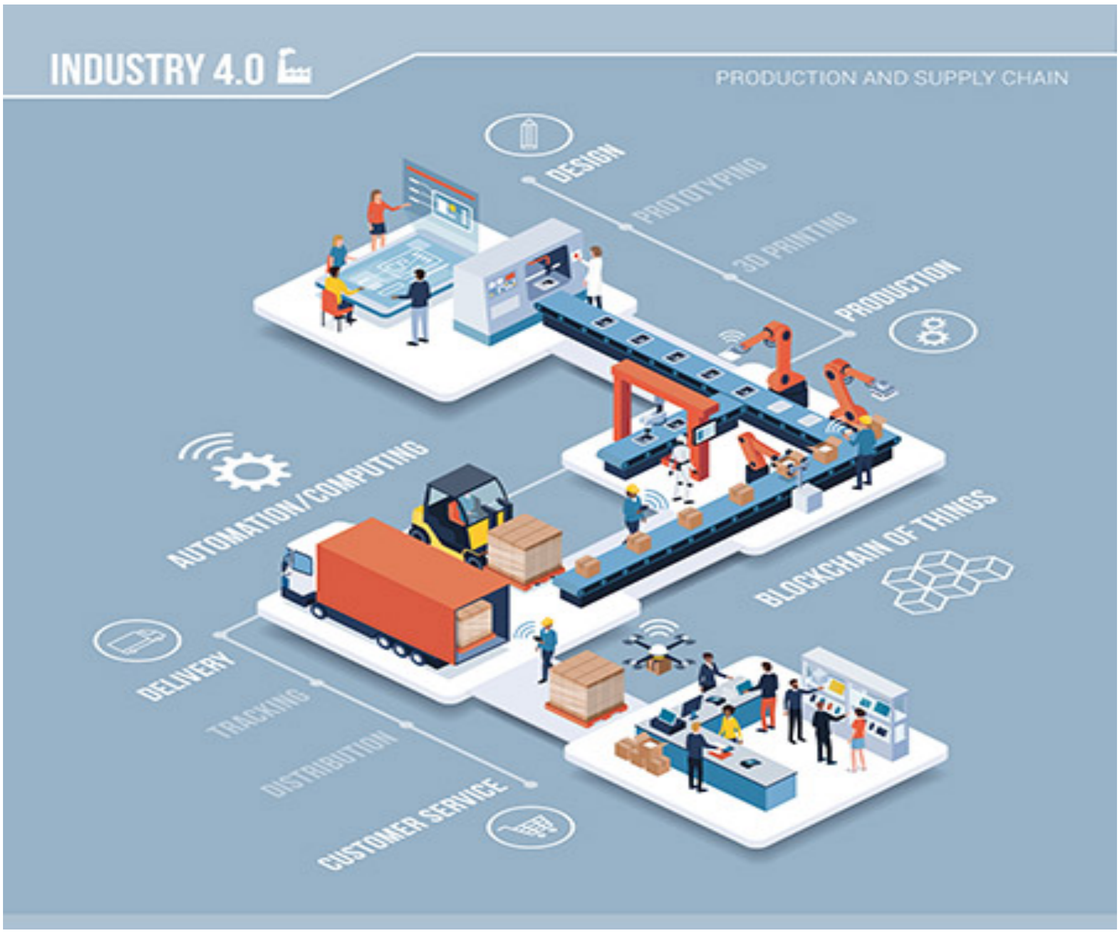


Figure 1: Industry 4.0

Industry 4.0 Technologies

Generally-speaking, Industry 4.0 describes the growing trend towards automation and data exchange in technology and processes within the manufacturing industry, including:

- The internet of things (IoT)
- The industrial internet of things (IIoT)
- Cyber-physical systems (CPS)
- Smart manufacture
- Smart factories
- Cloud computing
- Cognitive computing
- Artificial intelligence

This automation creates a manufacturing system whereby machines in factories are augmented with wireless connectivity and sensors to monitor and visualise an entire production process and make autonomous decisions.

Wireless connectivity and the augmentation of machines will be greatly advanced with the full roll out of 5G. This will provide faster response times, allowing for near real time communication between systems.

The fourth industrial revolution also relates to digital twin technologies. These digital technologies can create virtual versions of real-world installations, processes and applications. These can then be robustly tested to make cost-effective decentralised decisions.

These virtual copies can then be created in the real world and linked, via the internet of things, allowing for cyber-physical systems to communicate and cooperate with each other and human staff to create a joined up real time data exchange and automation process for Industry 4.0 manufacturing.

This automation includes interconnectivity between processes, information transparency and technical assistance for decentralised decisions.

In short, this should allow for digital transformation. This will allow for automated and autonomous manufacturing with joined-up systems that can cooperate with each other.

The technology will help solve problems and track processes, while also increasing productivity.

Example of the Industry 4.0 Revolution

Industry 4.0 has already been demonstrated through business models such as offline programming and adaptive control for arc welding, taking the process from product design through simulation and onto the shop floor for production.

There are also examples of businesses implementing Industry 4.0 in automotive manufacture and a variety of smart factories across the world.

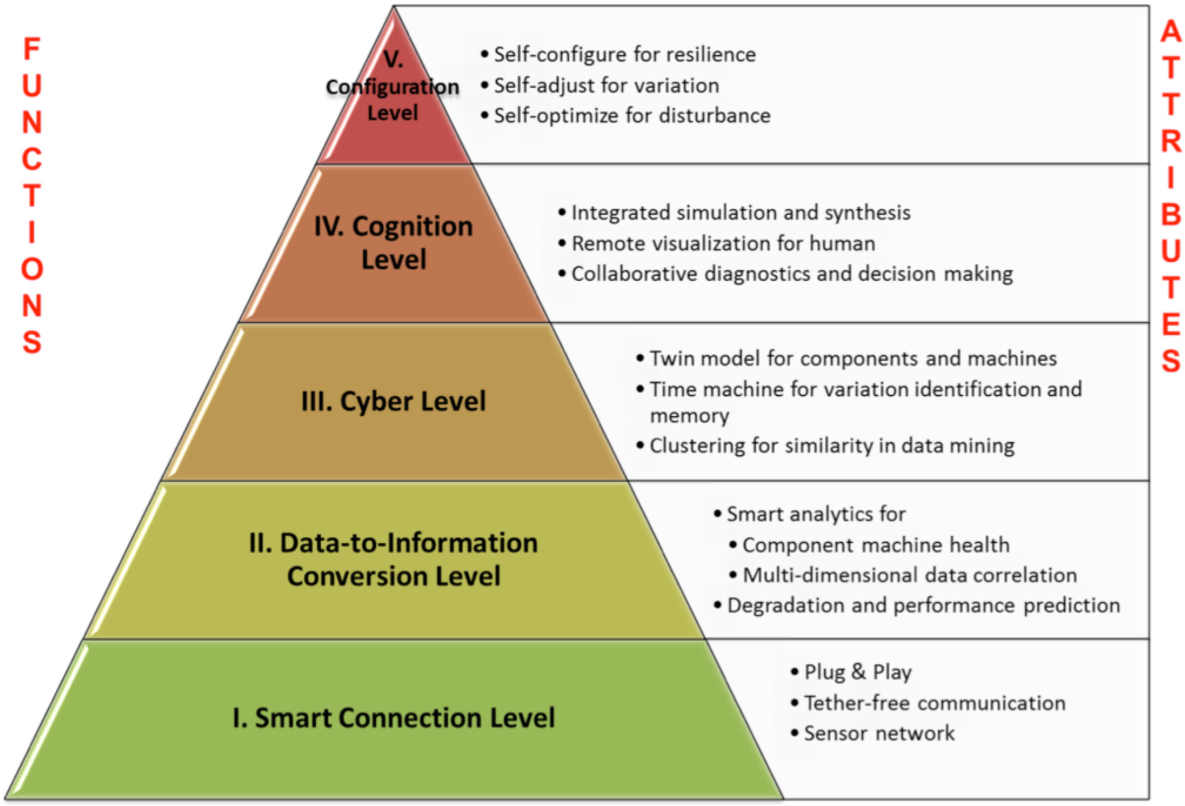


Figure 2: Industry 4.0 Revolution

A challenge in the development of embedded and cyber-physical systems is the large differences in the design practice between the various engineering disciplines involved, such as software and mechanical engineering. Additionally, as of today there is no "language" in terms of design practice that is common to all the involved disciplines in CPS. Today, in a marketplace where rapid innovation is assumed to be essential, engineers from all disciplines need to be able to explore system designs collaboratively, allocating responsibilities to software and physical elements, and analyzing trade-offs between them. Recent advances show that coupling disciplines by using co-simulation will allow disciplines to cooperate without enforcing new tools or design methods. Results from the MODELISAR project show that this approach is viable by proposing a new standard for co-simulation in the form of the Functional Mock-up Interface.

1.2 GLOBALIZATION AND EMERGING ISSUES

The threats of this crime have grown significantly as the process of globalization has expanded the levels and dimensions at which countries of the world interact nowadays. It appears that as the world becomes more globalized, the risk of cybercrime increases.

The official definition of "globalization" is the process by which businesses or other organizations develop international influence or start operating on an international scale.

More simply, globalization refers to an open flow of information, technology, and goods among countries and consumers. This openness occurs through various relationships, from business, geopolitics, and technology to travel, culture, and media.

Because the world is already so connected, most people don't notice globalization at work every single day. But the world is getting smaller, and companies need to understand what this means for the future of doing business. Companies that don't embrace globalization risk losing a competitive advantage, which allows other businesses to take over new opportunities in the global marketplace.

1.3 THE FOURTH REVOLUTION

Industry 4.0 is the digital transformation of manufacturing/production and related industries and value creation processes.

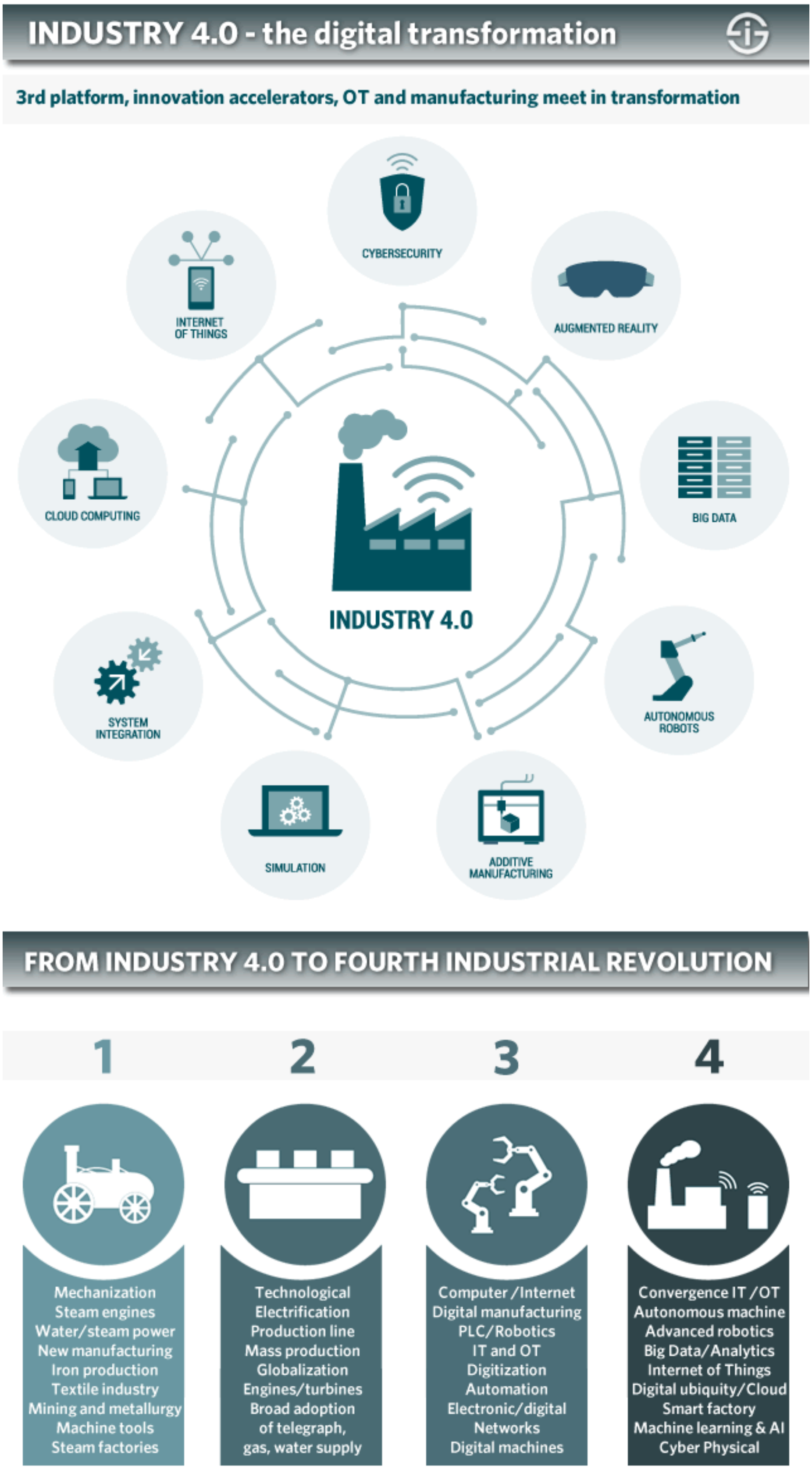


Figure 3: Industry 4.0 : The digital transformation

Industry 4.0 is used interchangeably with the fourth industrial revolution and represents a new stage in the organization and control of the industrial value chain.

Cyber-physical systems form the basis of Industry 4.0 (e.g., ‘smart machines’). They use modern control systems, have embedded software systems and dispose of an Internet address to connect and be addressed via IoT (the Internet of Things).

Industry 4.0 has been defined as “a name for the current trend of automation and data exchange in manufacturing technologies, including cyber-physical systems, the Internet of things, cloud computing and cognitive computing and creating the smart factory”.

Industrie 4.0 refers to the intelligent networking of machines and processes for industry with the help of information and communication technology (PlattformIndustrie 4.0)

Industry 4.0 is a vision that evolved from an initiative to make the German manufacturing industry more competitive *(‘Industrie 4.0’)* to a globally adopted term.

Industry 4.0 is often used interchangeably with the notion of the fourth industrial revolution. It is characterized by, among others,

- even more automation than in the third industrial revolution,
- the bridging of the physical and digital world through cyber-physical systems, enabled by Industrial IoT*,*
- a shift from a central industrial control system to one where smart products define the production steps,
- closed-loop data models and control systems and
- personalization/customization of products.

The goal is to enable autonomous decision-making processes, monitor assets and processes in real-time, and enable equally real-time connected value creation networks through early involvement of stakeholders, and vertical and horizontal integration.

Industry 4.0 is a vision, policy, and concept in motion, with reference architectures, standardization and even definitions in flux.

The fourth industrial revolution and the impact of the drivers and technologies behind Industry 4.0 have been looked at from the perspective of various sectors after the concept was launched. This has led to more '4.0' terms, often based on academic work. Examples include Logistics 4.0 *(logistics and transportation)*, Construction 4.0 *(construction industry)*, Energy 4.0 *(energy and utilities industry)*, and more.

Most Industry 4.0 initiatives are early-stage projects with a limited scope. The majority of digitization and digitalization efforts, in reality, happen in the context of third and even second industrial revolution technologies/goals.

In essence, the technologies making Industry 4.0 possible leverage existing data and ample additional data sources, including data from connected assets to gain efficiencies on multiple levels, transform existing manufacturing processes, create end-to-end information streams across the value chain and realize new services and business models.

To understand Industry 4.0, it is essential to see the full value chain which includes suppliers and the origins of the materials and components needed for various forms of smart manufacturing, the end-to-end digital supply chain and the final destination of all manufacturing/production, regardless of the number of intermediary steps and players: the end customer.

Enabling more direct models of personalized production, servicing, as well as customer/consumer interaction *(including gaining real-time data from actual product usage)* and cutting the inefficiencies, irrelevance and costs of intermediaries in a digital supply chain model, where possible, are some goals of Industry 4.0 in this customer-centric sense of increasingly demanding customers who value speed, *(cost)* efficiencies and value-added innovative services.

In the end, it remains business – with the innovative twist of innovation and transformation of business models and processes: increase profit, decrease costs, enhance customer experience, optimize customer lifetime value and where possible customer loyalty, sell more, and innovate to grow and remain relevant.

At the very core Industry 4.0 includes the (partial) transfer of autonomy and autonomous decisions to cyber-physical systems and machines, leveraging information systems.

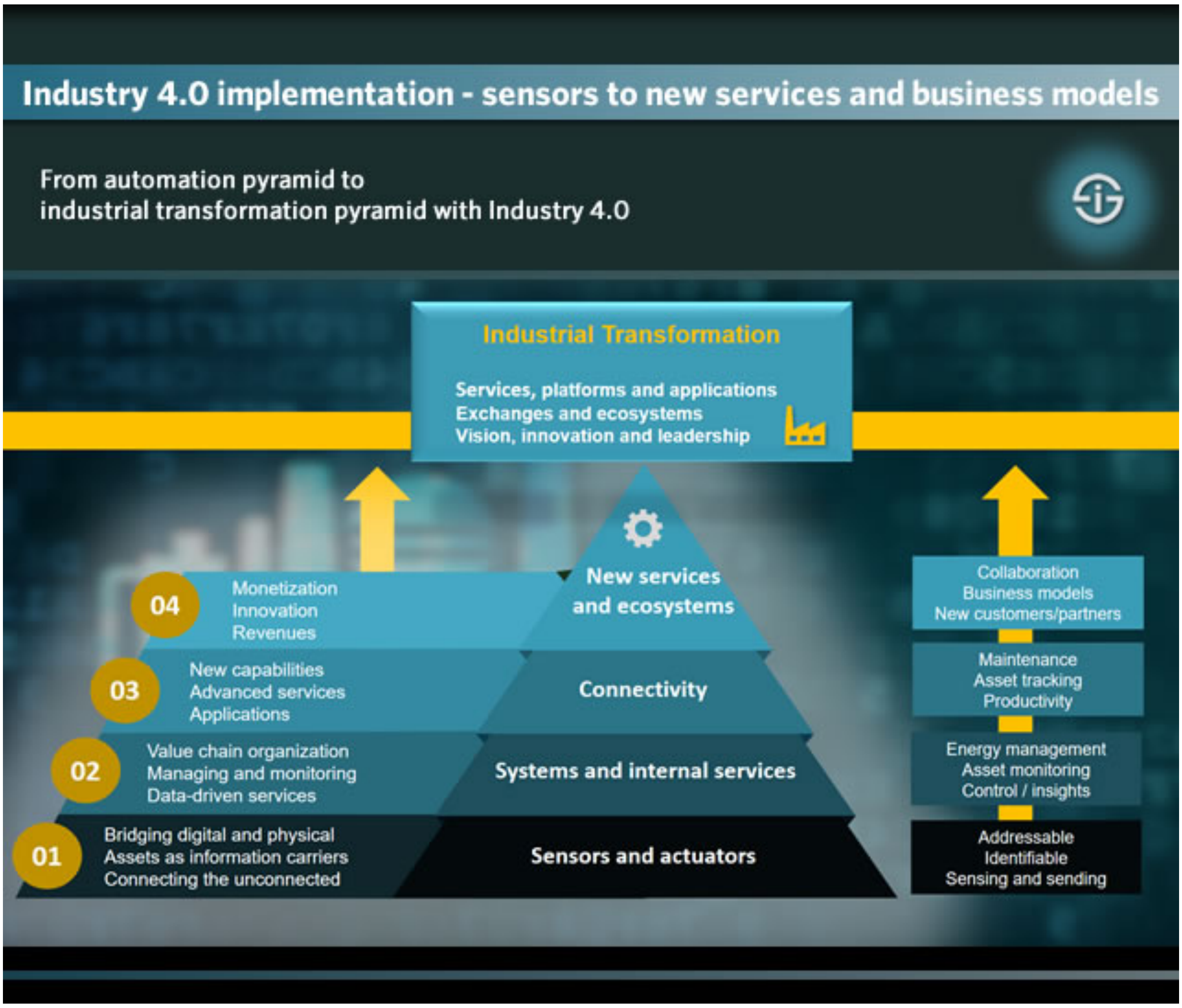


Figure 4: Industry 4.0 Implementation – sensors to new services and business models

Industry 4.0 is the information-intensive transformation of manufacturing (and related industries) in a connected environment of big data, people, processes, services, systems and IoT-enabled industrial assets with the generation, leverage and utilization of actionable data and information as a way and means to realize smart industry and ecosystems of industrial innovation and collaboration.

So, Industry 4.0 is a broad vision with clear frameworks and reference architectures, mainly characterized by the bridging of physical industrial assets and digital technologies in so-called cyber-physical systems.

A key role is indeed played by the Internet of Things or IoT, in the scope of Industry 4.0 Industrial IoT with its many IoT stack components, from IoT platforms to Industrial IoT gateways, devices and much more.

Yet, it’s not just IoT of course: cloud computing (and cloud platforms), big data (advanced data analytics, data lakes, edge intelligence) with (related) artificial intelligence, data analysis, storage and compute power at the edge of networks (edge computing), mobile, data communication/network technologies, changes on the level of, among others, HMI and SCADA, manufacturing execution systems (MES), enterprise resource planning (ERP, becoming i-ERP), programmable logic controllers (PLC), sensors and actuators, MEMS and transducers (sensors again) and innovative data exchange models all play a key role.

Additionally, the same technologies, such as Robotic Process Automation (RPA), AI (AI engines, machine learning), the meeting of both and so forth that pop up in close to all software areas such as enterprise information management, business process management and applications in the sourcing market are of course showing in IoT-enabled industrial/manufacturing applications and IoT manufacturing platforms as well.

Industry 4.0 is not ‘something’ you realize overnight. Just as is the case with IoT deployments you need a strategic and staged approach.

This is exactly the same as with digital transformation strategy and gets covered in depth when we look at Industry 4.0 strategy and implementation and at the state of Industry 4.0 and maturity of organizations as they move from initial stages and pilots to more innovative approaches on top of the traditional low-hanging fruit in terms of optimization and automation.

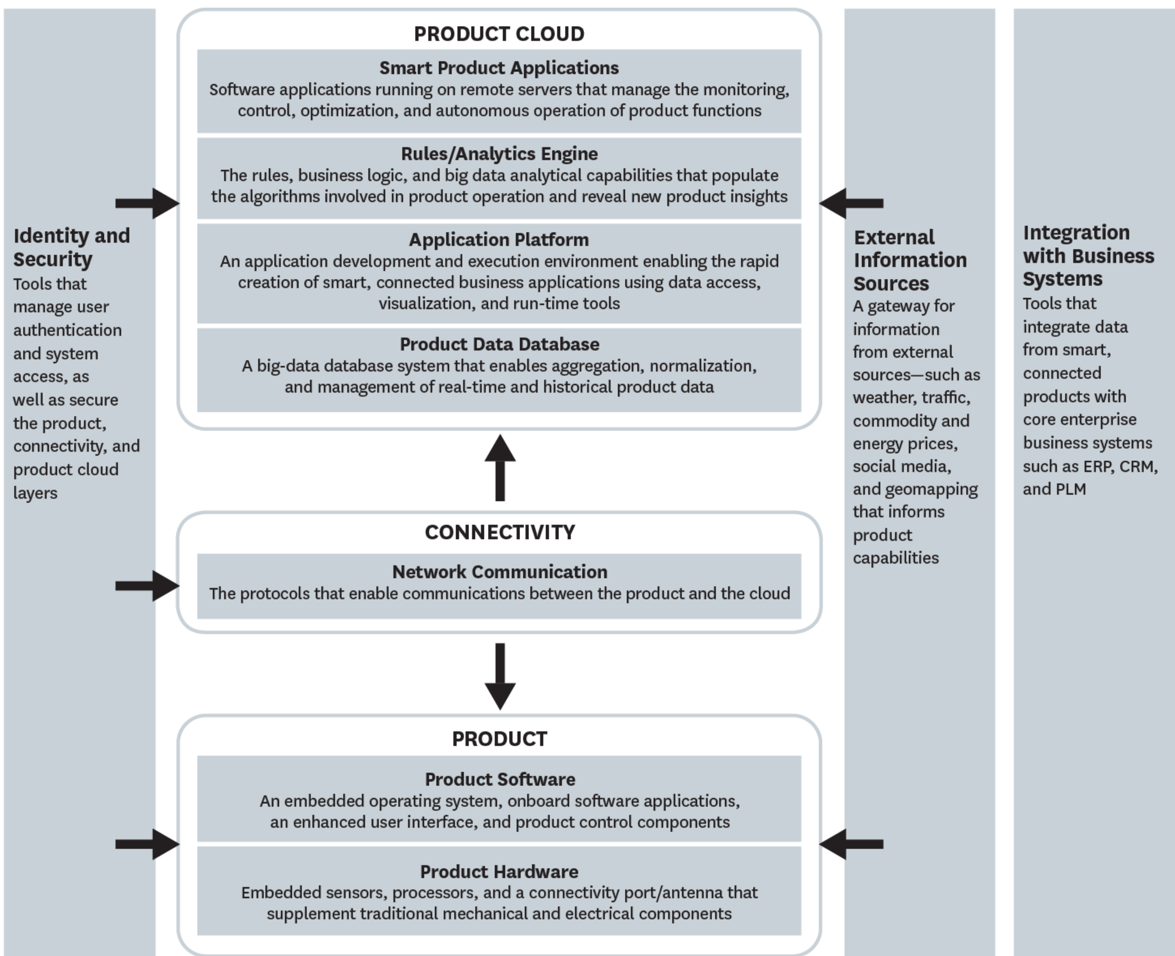
1.4 SMART AND CONNECTED BUSINESS PERSPECTIVE

The evolution of products into intelligent, connected devices—which are increasingly embedded in broader systems—is radically reshaping companies and competition.

Smart thermostats control a growing array of home devices, transmitting data about their use back to manufacturers. Intelligent, networked industrial machines autonomously coordinate and optimize work. Cars stream data about their operation, location, and environment to their makers and receive software upgrades that enhance their performance or head off problems before they occur. Products continue to evolve long after entering service. The relationship a firm has with its products—and with its customers—is becoming continuous and open-ended.

All smart, connected products, from home appliances to industrial equipment, share three core elements: *physical* components (such as mechanical and electrical parts); *smart* components (sensors, microprocessors, data storage, controls, software, an embedded operating system, and a digital user interface); and *connectivity* components (ports, antennae, protocols, and networks that enable communication between the product and the product cloud, which runs on remote servers and contains the product's external operating system).

Smart, connected products require a whole new supporting technology infrastructure. This "technology stack" provides a gateway for data exchange between the product and the user and integrates data from business systems, external sources, and other related products. The technology stack also serves as the platform for data storage and analytics, runs applications, and safeguards access to products and the data flowing to and from them.

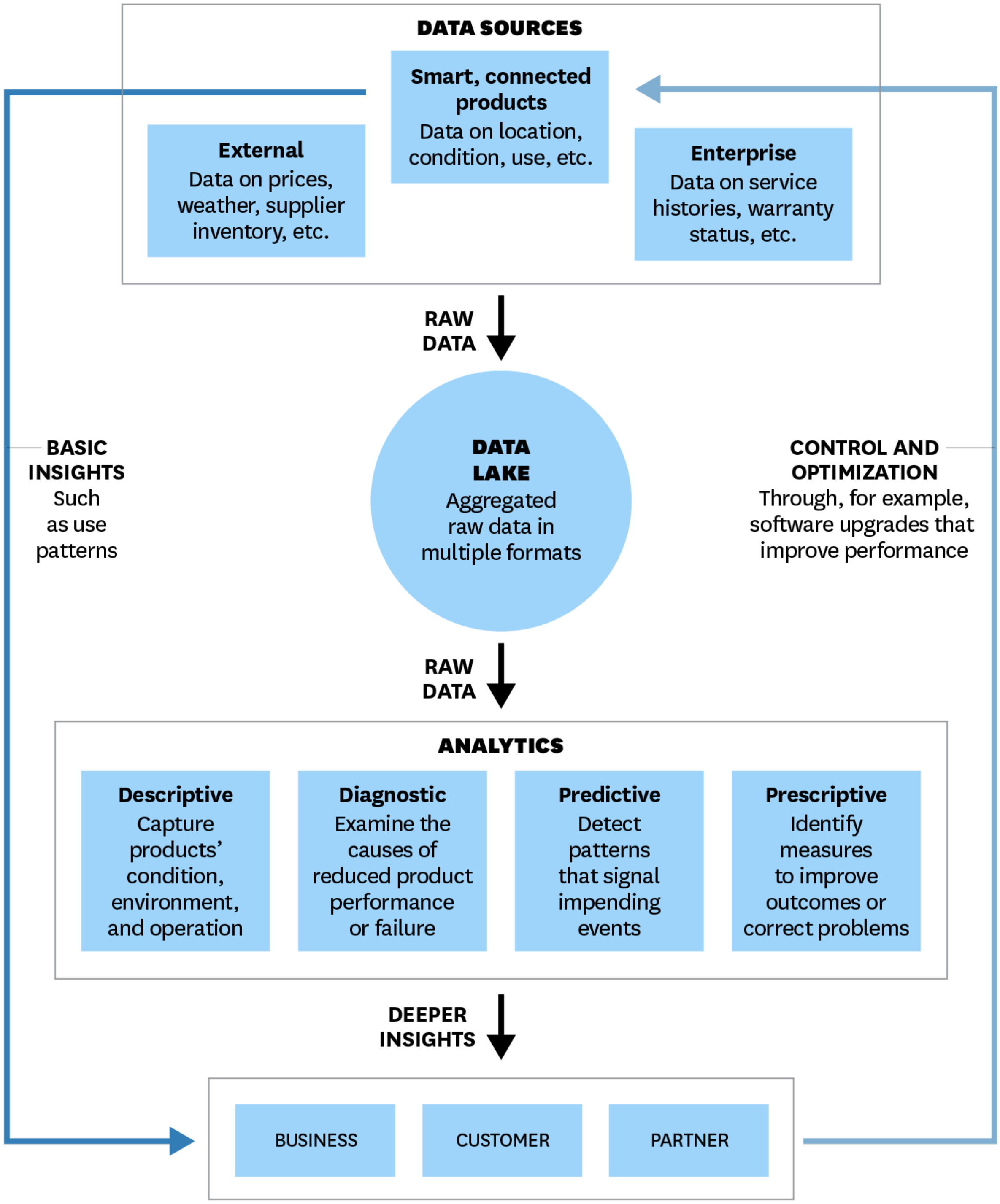


First, products can *monitor* and report on their own condition and environment, helping to generate previously unavailable insights into their performance and use. Second, complex product operations can be *controlled* by the users, through numerous remote-access options. That gives users the unprecedented ability to customize the function, performance, and interface of products and to operate them in hazardous or hard-to-reach environments.

Third, the combination of monitoring data and remote-control capability creates new opportunities for *optimization.* Algorithms can substantially improve product performance, utilization, and uptime, and how products work with related products in broader systems, such as smart buildings and smart farms. Fourth, the combination of monitoring data, remote control, and optimization algorithms allows *autonomy.* Products can learn, adapt to the environment and to user preferences, service themselves, and operate on their own.

Creating New Value with Data

Data from smart, connected products is generating insights that help businesses, customers, and partners optimize product performance. Simple analytics, applied by individual products to their own data, reveal basic insights; more-sophisticated analytics, applied to product data that has been pooled into a "lake" with data from external and enterprise sources, unearth deeper insights.



SOURCE MICHAEL E. PORTER AND JAMES E. HEPPELMANN
FROM "HOW SMART, CONNECTED PRODUCTS ARE TRANSFORMING COMPANIES," OCTOBER 2015

1.5 BASICS OF INDUSTRIAL IOT –

Industrial Internet of Things (IIoT)

IIoT is the use of those connected technologies to enhance manufacturing and industrial processes. It utilizes software, sensors, data systems, and more in manufacturing to improve speed, efficiency, and business performance.

The worldwide market for the IoT was $16.3 billion in 2016 but is expected to reach $185.9 billion by 2023, illustrating the relevancy of IoT for all industries during the coming years and decades.

MachineDesign.com, a technical resource created primarily for mechanical engineers, offers some examples of common IIoT use cases available today:

- **Preventive maintenance**: Records and communicates run-times or equipment cycles to avoid or predict asset downtime before it happens.
- **Predictive maintenance**: Provides warnings for conditions that indicate impending failure.
- **Energy consumption monitoring**: Provides power-consumption rates and assists in decisions to adjust equipment power usage to avoid peak-use energy penalties.
- **In-line quality sensors**: Delivers real-time data to the quality-assurance department to reduce labor for regulatory sampling, allowing for quick reaction to quality issues with raw materials or finished products.
- **Batch optimization**: Gives process engineers batch data and trends to optimize product production, "including improvements to mixing, heating, and cleaning times."
- **Proportional-integral-derivative (PID) loop tuning**:Time-series process data used for "PID loop-tuning improvements, mechanical performance issues of control valves, or finding root causes of process variations."
- **Inventory planning assistance**: Offers real-time inventory information, which can improve scheduling, shipping, and raw materials and finished goods ordering.

How to Get Started with IIoT

With potential IIoT use cases across an entire manufacturing process, it can be overwhelming to know where to start.

Start with a Problem

A common misconception is that IIoT adoption is not worth the cost or effort. An IIoT solution, as the word *solution* signifies, must *solve a problem*.

Consider:

- Does your facility run at 100% efficiency? If not, where are the breakdowns?
- Do you ever experience unscheduled downtime? Why?
- If communication breakdowns occur, where do they happen?

In any of those situations, IIoT can help. The key is to identify a problem, then assess IIoT solutions that can alleviate it.

When we talk to manufacturers, misconceptions or a lack of awareness about this emerging technology turn them off to the possibility of integration. Another common concern is that manufactures believe they won't be able to calculate an ROI.

Address Cybersecurity Risks

As you add IIoT devices to your manufacturing network, it becomes increasingly important to manage your cybersecurity.

Cybersecurity risks are inherent concerns of IIoT. Circumventing the problem first requires awareness that it exists. Horror stories of IIoT cybersecurity breaches result from a lack of awareness, planning and training.

A manufacturing-specific report addresses this concern by providing preventive measures you can use to reduce your potential risk, including:

- Penetration testing
- Ongoing system optimization/security patches
- Employee training and testing on safe Internet and system use
- Knowing who has access to internal systems and critical information
- Monitoring activity logs to identify patterns of abuse
- Having a clear plan and process for dealing with cyber security breaches, such as “what-if” scenarios to determine how you’ll address potential issues

1.6 INDUSTRIAL PROCESSES –

Industrial processes are procedures involving chemical, physical, electrical or mechanical steps to aid in the manufacturing of an item or items, usually carried out on a very large scale. Industrial processes are the key components of heavy industry.

Challenges in industrial process control

The heterogeneity in cyber-physical systems exposes several problems that cannot be easily solved through current control, communications, and software theory. As an example, today's network research often deals with coverage and connectivity issues assuming homogeneous network components. However, coverage and connectivity should clearly be redefined in cyberphysical control network systems. Such systems will consist of wired and wireless networks with different capacities and reliability. To model such heterogeneous network systems, a rethinking of network technology is necessary.

Cyber-physical systems also put emphasis on real-time operations. Sensing, processing, communication and actuation in the control loops are handled by different components in the network. For example, a control loop can be easily designed for an optical quality monitoring system with bounded image processing time to determine if the product should be picked out due to optical defects. However, in large-scale control networks, handling the network events such as routing, verifying and retransmitting messages may consume unpredictable time if the network protocol is not designed with timing issues in mind.

To the best of our knowledge, there is not much work done towards a unifying theory for large-scale problems in industry process control. On the contrary, different subsystems of a production processing line are generally isolated. Moreover, traditional control theory lacks the necessary tools to analyze interconnected systems of heterogeneous components in large scale. Hence, it is difficult to provide real-time and reliability guarantees without revisiting communication and control theory.

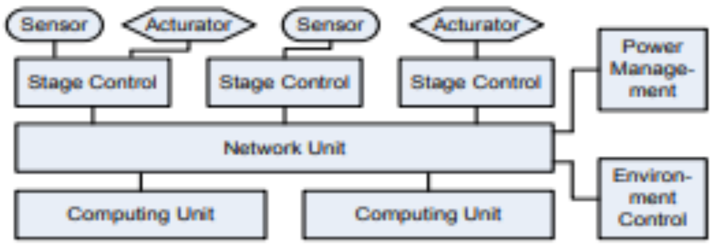


Figure 1. Proposed CPS architecture

Figure 5: Proposed CPS architecture

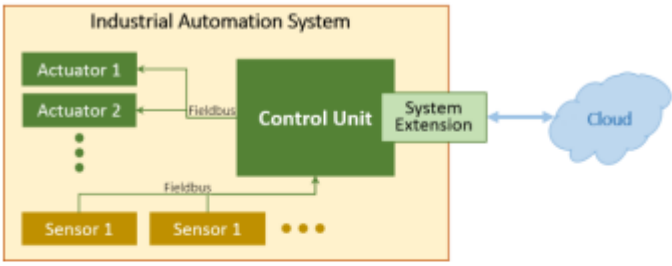


Fig. 1. Figure 1: Direct system control

Figure 6: Direct System Control

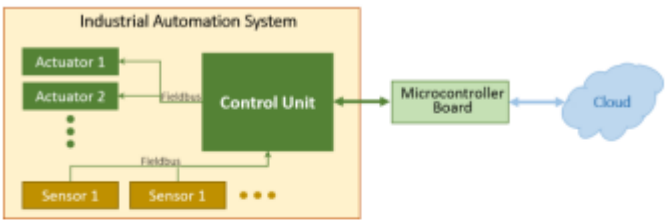


Fig. 2. System extension by microcontroller board

Figure 7: System Extension by microcontroller board

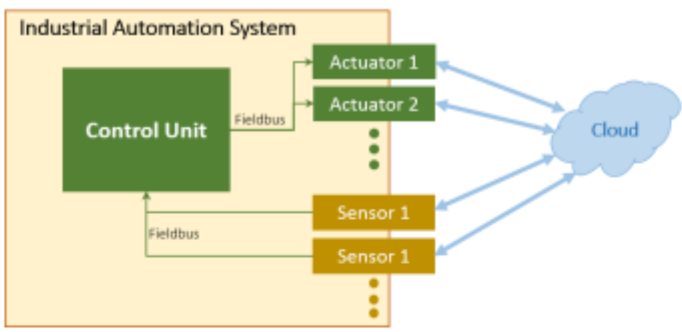


Fig. 3. Usage of intelligent actuators and sensors

Figure 8: Usage of intelligent actuators and sensors

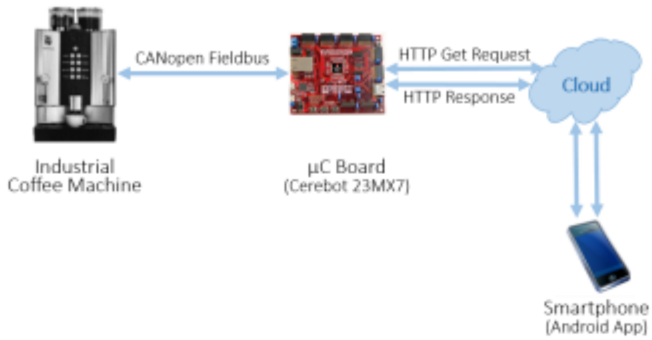


Fig. 4. System architecture

Figure 9: System Architecture of Industrial Coffee Maker

1.7 INDUSTRIAL SENSING AND ACTUATION

The Internet of Things is a major contributing factor to the new Data Economy. The value of an IoT system goes beyond the originally intended use case, for instance in automation. This is because the further value lies in the intelligence that an IoT system creates. Sensors are the source of IoT data and sensors and actuators in IoT can work together to enable automation at an industrial scale. Finally, analysis of the data that these sensors and actuators produce can provide valuable business insights over time.

What are the main sensors and actuators?

Sensors and actuators often work in tandem, but they are essentially opposite devices. A sensor monitors conditions and signals when changes occur. An actuator receives a signal and performs an action, often in the form of movement in a mechanical machine. Another key difference is their location within the system.

Driven by new innovations in materials and nanotechnology, sensor technology is developing at a never-before-seen pace, resulting in increased accuracy, decreased size and cost, and the ability to measure or detect things that weren't previously possible. In fact, sensing technology is advancing so rapidly that we will see a trillion new sensors deployed annually within a few years.

Sensors

A better term for a sensor is a transducer. A transducer is any physical device that converts one form of energy into another. So, in the case of a sensor, the transducer converts some physical phenomenon into an electrical impulse that determines the reading. A microphone is a sensor that takes vibrational energy (sound waves) and converts it to electrical energy in a useful way for other components in the system to correlate back to the original sound.

Actuators

Another type of transducer that you will encounter in many IoT systems is an actuator. In simple terms, an actuator operates in the reverse direction of a sensor. It takes an electrical input and turns it into physical action. For instance, an electric motor, a hydraulic system, and a pneumatic system are all different types of actuators.

Controller

In a typical IoT system, a sensor may collect information and route it to a control center. There, previously defined logic dictates the decision. As a result, a corresponding command controls an actuator in response to that sensed input. Thus, sensors and actuators in IoT work together from opposite ends.

IoT Variety is Key

There are many different types of sensors in an IoT system. Flow sensors, temperature sensors, voltage sensors, humidity sensors, and the list goes on. In addition, there are multiple ways to measure the same thing. For instance, a small propeller similar to the one you see on a weather station can measure airflow. However, this method would not work in a moving vehicle. As an alternative, vehicles can measure airflow by heating a small element and measuring the rate at which it cools.

Different applications call for different ways of measuring the same thing. At the same time, a single variable could trigger multiple actions. As a result, sensors and actuators in IoT must work together reliably.

The Importance of Accurate Sensors

Imagine that you are a bar owner and you want to measure the amount of beer coming out of one of your taps. One way you might do this is to install a sensor in a line that runs from the keg of beer to the tap. This sensor would most likely have a small impeller inside of it.

When the beer ran through the sensor, it would cause the impeller to spin, just like the propeller on a weather station.

When the impeller spins, it will send a stream of electrical impulses to a computer. The computer will interpret the impulses to determine how much beer is flowing through. Sounds simple, right?

This is where sensors get interesting. If you look back at our description, you'll see that we never directly measured the amount of beer flowing through the sensor; we interpreted it from a stream of electrical impulses. That means that we must first figure out how to interpret it.

Sensor Calibration

To calibrate the sensor, we'd have to take a container with a known carrying capacity, say, a pint glass. Then we'd have to fill that container under a variety of conditions to determine what the electrical pulse signal looked like. Then, monitor the actuator that is responsible to turn on and off the flow on the other end.

For instance, the first pour off a new keg might tend to have more foam, which would read differently than a pour from the middle of the keg that was all beer. It's only through repeated trials and a lot of data that we gain the confidence of interpreting the data. Sensors and actuators in IoT can work together to automate processes, such as filling bottles.

The Importance of Accurate Calibration

With this correlation identified, a protocol can always assure the sensor is reading correctly. This process is calibration. Reputable manufacturers will deliver fully calibrated devices and provide instruction on how to re-calibrate to verify sensor accuracy.

The accuracy of sensed data is paramount since you will make mission-critical decisions based on later analysis of the data, which will hold little value if the data is wrong.

Another Example:

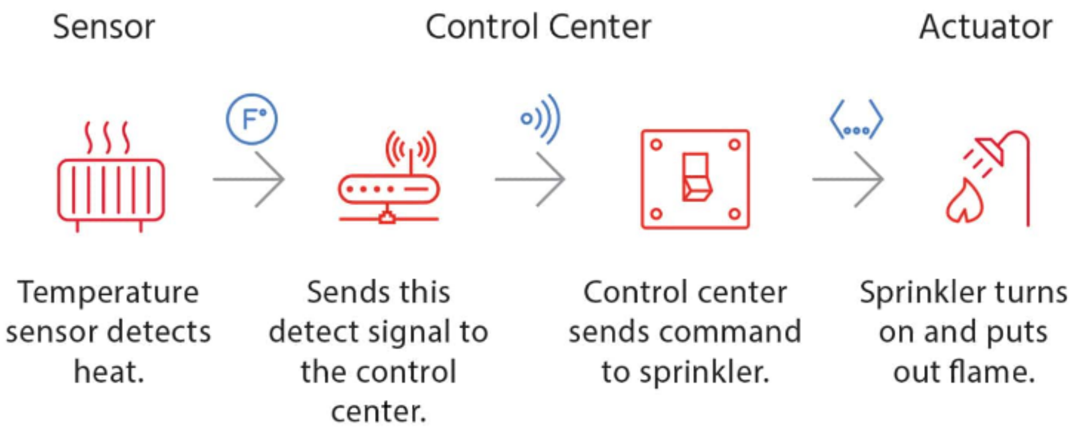


Figure 10:

Types of Sensors Used in Industrial Automation

Temperature Sensors :

A temperature sensor is a device that collects information concerning the temperature from a resource and changes it to a form that can be understood by another device. These are commonly used category of sensors which detect Temperature or Heat and it also measures the temperature of a medium.

Digital Temperature Sensors and Humidity & Temperature Sensors are few of the main temperature sensors used in automation.

Digital Temperature Sensors:

These Digital Temperature Sensors are silicon-based temperature- sensing ICs that provide accurate output through digital representations of the temperatures they are measuring. This simplifies the control system's design, compared to approaches that involve external signal conditioning and an analog-to digital converter (ADC).

Humidity & Temperature Sensors

The Temperature & Humidity sensors attribute a temperature & humidity sensor complex with a measured digital signal output. By utilizing the technique and temperature & limited digital-signal-acquisition humidity sensing technology, it ensures high consistency and exceptional long-standing stability.

Applications of Temperature Sensors:

- They are weatherproof & designed for continuous temperature measurement in air, soil, or water
- Exceptional accuracy and stability
- For measurements in complex industrial applications
- For measurements under rough operating conditions

Pressure Sensors:

The Pressure Sensor is an Instrument that apprehends pressure and changes it into an electric signal where the quantity depends upon the pressure applied.

Turned parts for Pressure Sensors and Vaccum Sensors are few of the major pressure sensors used in Industrial automation.

Turned parts for Pressure Sensors

- 

These Pressure sensors are widely used in Industrial and hydraulic systems, these are high pressure industrial automation sensors also used in climate control systems.

- **Vaccum Sensors**

Vaccum Sensors are used when the Vaccum pressure is below atmospheric pressure levels and it can be difficult to sense through mechanical methods. These sensors generally depend on a heated wire with electrical resistance correlating to temperature. When vaccum pressure increases, convection falls down and wire temperature up rises. Electrical resistance increases proportionally and is calibrated adjacent to pressure in order to give an effective measurement of the vaccum.

Applications of Pressure Sensors:

- Used to measure pressure below than the atmospheric pressure at a given location
- Used in weather instrumentation, aircrafts, vehicles, and any other machinery that has pressure functionality implemented
- Pressure sensors can be used in systems to measure other variables such as fluid/gas flow, speed, water level, and altitude

Acceleration sensors

Micro-electro-mechanical Systems (MEMS) Acceleration Sensors are one of the main inertial sensors; and are dynamic sensor competent of have a greater range of sensing capabilities.

Motion sensors

Micro-electro-mechanical system (MEMS) motion sensors use data processing algorithms designed on a motion interaction platform which integrates numerous low-cost MEMS motion sensors with ZigBee wireless technology to carry personified interactions while working together with machines. Sensor signal processing systems mainly solve noise cancellation; signal smoothing, gravity influence partition, coordinate system alteration, and position information recovery .Widely used in the automotive Industry in ABS technology.

Applications of MEMS Sensors:

- These have numerous applications ranging from industry, entertainment, sports to education. For example, triggering airbag deployments or monitoring of nuclear reactors
- Used to measure static acceleration (gravity), tilt of an object, dynamic acceleration in an aircraft, shock to an object in a car, vibration of an object. Cell phones, washing machines or computers
- Used to detect motion

Torque sensors

The torque sensors complete with essential mechanical stops, raise overload capacity and offer additional guard during mounting and operation.

Rotating Torque & Torque Transducers are few important sensors used in industrial automation.

Rotating Torque Sensors

This Rotating Torque industrial automation sensors used for measuring reaction of rotating torque. These torque meters complete with essential mechanical stops increase surplus capacity and offer extra safety during mounting and operation.

Torque Transducers

These torque transducers utilize superior strain gage technology to indulge the most challenging necessities for static and dynamic applications of sensors.

Applications of Torque Sensors:

- Used to Measure the speed of rotation and maintenance necessities
- Used to measure Mass and mass moment of inertia
- The amount of the torque to be calculated, from the point of vision of quasi-static process
- Used to measure the highest speed of rotation, oscillating torque

1.8 INDUSTRIAL INTERNET SYSTEMS –

Industrial internet of things

The industrial internet of things (IIoT) is the use of smart sensors and actuators to enhance manufacturing and industrial processes. Also known as the industrial internet or Industry 4.0, IIoT uses the power of smart machines and real-time analytics to take advantage of the data that "dumb machines" have produced in industrial settings for years. The driving philosophy behind IIoT is that smart machines are not only better than humans at capturing and analyzing data in real time, but they're also better at communicating important information that can be used to drive business decisions faster and more accurately.

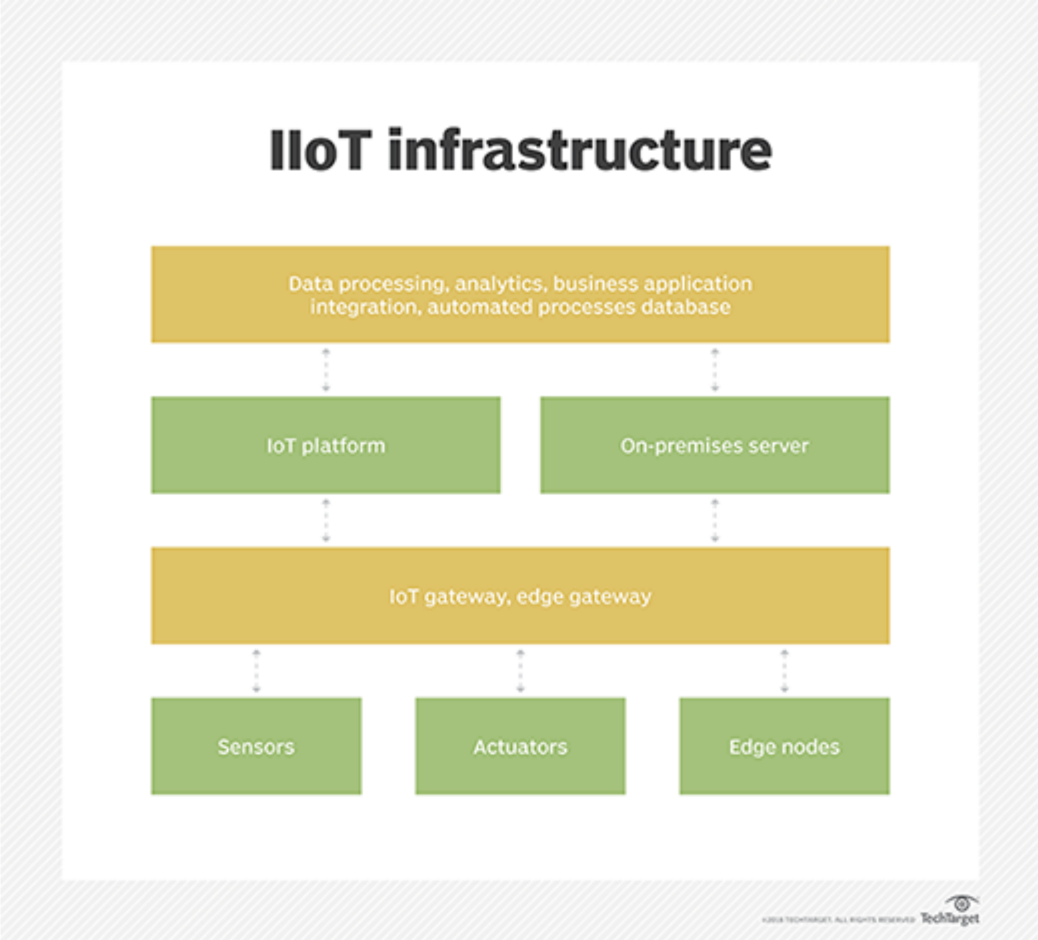
Connected sensors and actuators enable companies to pick up on inefficiencies and problems sooner and save time and money, while supporting business intelligence efforts. In manufacturing, specifically, IIoT holds great potential for quality control, sustainable and green practices, supply chain traceability, and overall supply chain efficiency. In an industrial setting, IIoT is key to processes such as Predictive maintenance (PdM), enhanced field service, energy management and asset tracking.

IIoT working

IIoT is a network of intelligent devices connected to form systems that monitor, collect, exchange and analyze data. Each industrial IoT ecosystem consists of:

- connected devices that can sense, communicate and store information about themselves;
- public and/or private data communications infrastructure;
- analytics and applications that generate business information from raw data;
- storage for the data that is generated by the IIoT devices; and
- people.

These edge devices (An edge device is any piece of hardware that controls data flow at the boundary between two networks)and intelligent assets transmit information directly to the data communications infrastructure, where it's converted into actionable information on how a certain piece of machinery is operating. This information can be used for predictive maintenance, as well as to optimize business processes.



Industries usingIIoT

There are countless industries that make use of IIoT. One example is the automotive industry, which uses IIoT devices in the manufacturing process. The automotive industry extensively uses industrial robots, and IIoT can help proactively maintain these systems and spot potential problems before they can disrupt production.

The agriculture industry makes extensive use of IIoT devices, too. Industrial sensors collect data about soil nutrients, moisture and more, enabling farmers to produce an optimal crop.

The oil and gas industry also uses industrial IoT devices. Some oil companies maintain a fleet of autonomous aircraft that can use visual and thermal imaging to detect potential problems in pipelines. This information is combined with data from other types of sensors to ensure safe operations.

Benefits of IIoT

One of the top touted benefits of IIoT devices used in the manufacturing industry is that they enable predictive maintenance. Organizations can use real-time data generated from IIoT systems to predict when a machine will need to be serviced. That way, the necessary maintenance can be performed before a failure occurs. This can be especially beneficial on a production line, where the failure of a machine might result in a work stoppage and huge costs. By proactively addressing maintenance issues, an organization can achieve better operational efficiency.

Another benefit is more efficient field service. IIoT technologies help field service technicians identify potential issues in customer equipment before they become major issues, enabling techs to fix the problems before they inconvenience customers. These technologies might also provide field service technicians with information about which parts they need to make a repair. That way, the technician has the necessary parts with them when making a service call.

Asset tracking is another IIoT perk. Suppliers, manufacturers and customers can use asset management systems to track the location, status and condition of products throughout the supply chain. The system sends instant alerts to stakeholders if the goods are damaged or at risk of being damaged, giving them the chance to take immediate or preventive action to remedy the situation.

IIoT also allows for enhanced customer satisfaction. When products are connected to the internet of things, the manufacturer can capture and analyze data about how customers use their products, enabling manufacturers and product designers to build more customer-centric product roadmaps.

IIoT also improves facility management. Manufacturing equipment is susceptible to wear and tear, which can be exacerbated by certain conditions in a factory. Sensors can monitor vibrations, temperature and other factors that might lead to suboptimal operating conditions.

Is IIoT secure?

Early on, manufacturers created IoT devices with little regard for security, resulting in a perception that IoT devices are inherently insecure. Given the similarities between IoT and IIoT devices, it's worth considering whether it's safe to use IIoT devices.

As with any other connected device, IIoT devices must be evaluated on a device-by-device basis. It's entirely possible that one manufacturer's device is secure while another isn't. Even so, security is a bigger priority among device manufacturers than ever before.

In 2014, several technology companies including AT&T, Cisco, General Electric, IBM and Intel came together to form the Industrial Internet Consortium (IIC). Although this group's primary objective is to accelerate the adoption of IIoT and related technologies, it's making security a priority, even going so far as to form a security working group. The IIC's other working groups include Technology, Liaison, Marketing, Industry and Digital Transformation.

Risks and challenges of IIoT

The biggest risks associated with IIoT use pertain to security. It's relatively common for IIoT devices to continue using default passwords, even after they have been placed into production. Similarly, many IIoT devices transmit data as clear text. These conditions would make it relatively easy for an attacker to intercept the data coming from an IIoT device. Similarly, an attacker could take over an insecure IIoT device and use it as a platform for launching an attack against other network resources.

Security is a big challenge for those who are responsible for an organization's IIoT devices, but so, too, is device management. As an organization adopts more and more IIoT devices, it will become increasingly important to adopt an effective device management strategy. More specifically, organizations must be able to positively identify IIoT devices to prevent the use of rogue devices. Establishing a means of identifying each individual device is also crucial for tasks such as replacing a failed device or performing a device refresh.

Patch management presents another big challenge regarding IIoT devices. It's becoming increasingly common for device manufacturers to issue periodic firmware updates. Organizations must have an efficient means of checking devices to see if they have the latest firmware installed and deploying new firmware if necessary. Additionally, such a tool must adhere to the organization's established maintenance schedule so as to not disrupt operations.

Difference between IoT and IIoT

Although IoT and IIoT have many technologies in common, including cloud platforms, sensors, connectivity, machine-to-machine communications and data analytics, they are used for different purposes.

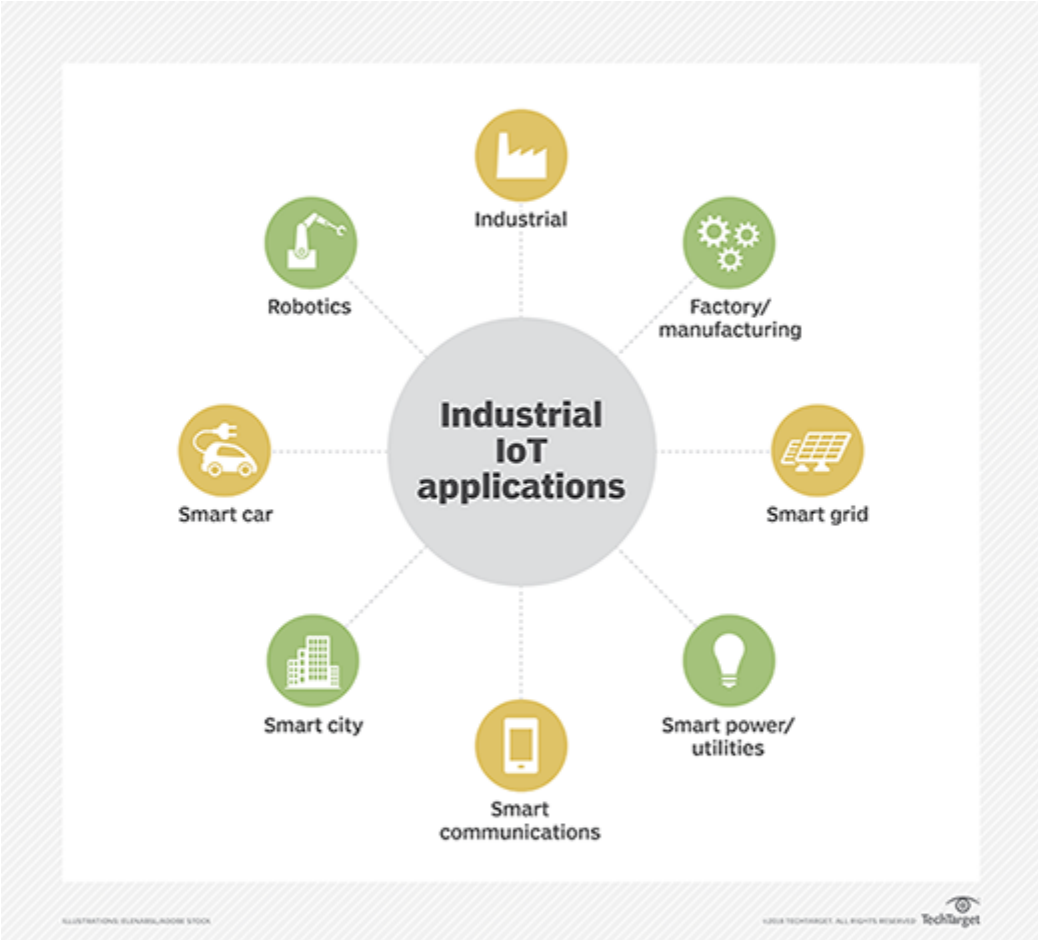
IoT applications connect devices across multiple verticals, including agriculture, healthcare, enterprise, consumer and utilities, as well as government and cities. IoT devices include smart appliances, fitness bands and other applications that generally don't create emergency situations if something goes amiss.

IIoT applications, on the other hand, connect machines and devices in such industries as oil and gas, utilities and manufacturing. System failures and downtime in IIoT deployments can result in high-risk situations, or even life-threatening ones. IIoT applications are also more concerned with improving efficiency and improving health or safety, versus the user-centric nature of IoT applications.

IIoT applications and examples

In a real-world IIoT deployment of smart robotics, ABB, a power and robotics firm, uses connected sensors to monitor the maintenance needs of its robots to prompt repairs before parts break.

Likewise, commercial jetliner maker Airbus has launched what it calls the *factory of the future*, a digital manufacturing initiative to streamline operations and boost production. Airbus has integrated sensors into machines and tools on the shop floor and outfitted employees with wearable tech -- e.g., industrial smart glasses -- aimed at cutting down on errors and enhancing workplace safety.



IIoT is used in many industries and sectors, including robotics, manufacturing and smart cities.

Another robotics manufacturer, Fanuc, is using sensors in its robotics, along with cloud-based data analytics, to predict the imminent failure of components in its robots. Doing so enables the plant manager to schedule maintenance at convenient times, reducing costs and averting potential downtime.

Magna Steyr, an Austrian automotive manufacturer, is taking advantage of IIoT to track its assets, including tools and vehicle parts, as well as to automatically order more stock when necessary. The company is also testing "smart packaging" that is enhanced with Bluetooth to track components in its warehouses.

IIoT vendors

There are several vendors with IIoT platforms, including:

- **ABB Ability.** An IIoT company specializing in connectivity, software and machine intelligence.
- **Aveva Wonderware.** A company that develops human-machine interface (HMI) and IoT edge platforms for OEMs (original equipment manufacturers) and end users.

- **Axzon.** An IIoT company focusing on smart automotive manufacturing, predictive maintenance and cold chain.
- **Cisco IoT.** A networking company offering platforms for network connectivity, connectivity management, data control and exchange, and edge computing.
- **Fanuc Field System.** A company that has developed a platform for connecting various generations, makes and models of industrial IoT equipment.
- **Linx Global Manufacturing.** A product development and manufacturing company offering custom IIoT, application and data management platforms.
- **MindSphere by Siemens.** An industrial IoT solution based around artificial intelligence (AI) and advanced analytics.
- **Plataine.** An IIoT company specializing in using AI to generate actionable insights in manufacturing.
- **Predix by GE.** A platform for connecting, optimizing and scaling digital industrial applications.

IIoT and 5G

5G is the emerging standard for mobile networks. It has been specifically designed to deliver fast data throughput speeds with low latency. 5G will support download speeds of up to 20 Gbps (gigabits per second) with sub-millisecond latency.

The emergence of 5G will likely affect the use of IIoT devices in two main ways. First, 5G's high throughput and low latency will make it possible for devices to share data in real time. Previously, this was only possible when the devices were located on private networks with high-speed connectivity. This real-time connectivity will support use cases such as driverless cars and smart cities.

The other way 5G will affect IIoT adoption is that it will likely result in device proliferation. Industrial operations might use thousands of 5G connected devices. 5G's high speed and low latency also means we'll likely see IIoT devices used in remote sites whose lack of high-speed connectivity previously made IIoT use impractical.

Future of IIoT

The future of IIoT is tightly coupled with a trend known as Industry 4.0. Industry 4.0 is, essentially, the fourth Industrial Revolution.

Industry 1.0 was the first Industrial Revolution and occurred in the late 1700s as companies began to use water-powered or steam-powered machines in manufacturing. Industry 2.0 started at the beginning of the 20th century and was brought about by the introduction of electricity and assembly lines. Industry 3.0 occurred in the latter part of the 20th century and was tied to the use of computers in the manufacturing process.

Industry 4.0 is where we are today. Industry 4.0 is based on the use of connected electronic devices -- particularly, IIoT devices.

Going forward, IIoT devices will play a major role in digital transformations, especially as organizations attempt to digitize their production lines and supply chains. Additionally, big data analytics will evolve to incorporate IIoT data. This will make it possible for organizations to detect changing conditions in real time and respond accordingly.

Although IIoT devices have been around for several years, real-world adoption is still in its infancy. This is sure to change as 5G becomes increasingly prevalent and more and more organizations begin to realize what IIoT can do for them. There are a number of resources available online for organizations that want to get up to speed on IoT and IIoT.

https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT

1.9 BASIC PRINCIPLES OF DESIGN AND VALIDATION OF CPS

PRINCIPLES: INTEGRATING THE PHYSICAL AND CYBER

The core principle of CPS is the bridging of engineering and physical world applications and the computer engineering hardware and computer science cyber worlds. Basic principles of the physical world include elements of physics, modeling, and real-world intangibles such as uncertainty and risk. Concurrently, the principles of computer engineering and computer science worlds deal with embedded systems, networking, programming, and algorithms. CPS education thus goes beyond exposure to the traditional dynamical systems models (ordinary differential or difference equations) to an understanding of physical impacts not only at the physical layer, but also across the physical-cyber interface.

Sensors are an example of a hardware bridge between the physical and cyber worlds. They are the primary devices that collect data from the physical world that are then used as input to the cyber world. Understanding the properties and principles of sensors and how to use them in a manner that is aware of sensor and real-world constraints is critical. Unfortunately, high-level abstractions used to simplify system development often have the undesirable side effect of hiding key physical world principles that programmers need to know if the CPS they develop are to work properly. Once raw data are collected, they are processed via signal processing techniques. The required principles of signal processing include linear signals and systems theory, analog and digital filtering, time and frequency domain analysis, convolution, linear transforms like the discrete Fourier transform and fast Fourier transform, noise and statistical characterization of signals, machine learning, and decision and sensor fusion. In CPS, considerations of the implementations of these signal processing techniques on embedded CPUs, running in real time and with safety critical implications, are necessary, as is the topic of sensor reliability. Often these issues are not considered in classical signal processing courses.

Control is a central tenet of CPS. Relevant elements of control theory include stability and optimization as well as control techniques in the context of networks, hybrid systems, stochastic systems, and digital systems. Of particular importance in the cyber domain are the implications for control of distributed systems and the inherent delays they impose.

In today's networked, wireless, and real-time world, and as cyber-physical systems become embedded in our economy and society, knowledge of the principles underlying these topics is also necessary for CPS engineering. Areas where students need this knowledge include the following:

Communication and networking. CPS requires an understanding from physical-layer principles to protocols, layered architectures, and the many real-world properties of wireless communications.

Real time. An understanding of topics like real-time scheduling theory, temporal semantics in programs, and clock synchronization in networks is needed.

Distributed systems. The distributed and networked nature of CPS in many of the applications of interest should be included in CPS education. Even though distributed systems and networking are covered in traditional engineering or computer science curricula, these courses often do not address CPS issues. CPS combines the hardware implementation with the software that runs the algorithms, all operating in a natural world setting.

Embedded systems. A strong education and training on the principles of embedded software, the many principles of programming, algorithms, software design, formal methods, and platforms (architectures and operating systems) are necessary to enable the development of reliable and high-quality cyber components of a CPS system.

Physical properties. It is important to understand and be able to model the physical properties of the environments and hardware platforms. Software design principles that address the realisms of the physical world in such a way as to satisfy safety, reliability, real-time performance, risk management, and security requirements need to be part of the curriculum.

Human interaction. Human factors design, human-in-the-loop control, and understanding and accounting for the behavioral responses of humans are important for many CPS. One important design issue is making CPS easy for humans to operate, control, and maintain. Similar to other engineering disciplines, hands-on projects and interdisciplinary teamwork are also fundamental to understanding and seeing core principles applied.

FOUNDATIONS OF CPS

Drawing on these principles, the committee identified six key overarching foundations for a CPS curriculum (Box 2.1).

Foundation 1, basic computing concepts, is included to emphasize that the cyber expertise required cannot be achieved with only one or two programming classes; it can only be attained with solid training in computing that draws on examples and case studies from the physical domain. In particular, it is necessary to teach how the properties of thephysical world have to be addressed in the cyber world to achieve the system characteristics listed in the next subsection.

Foundation 2, computing for the physical world, highlights the need to include properties and constraints of the physical world. Real-world complexities often give rise to situations not addressed by the software, often resulting in failures; consequently, it is necessary to have a foundation in laws of the physical world. Software designs and implementations need to take into account the resource limitations of the platforms themselves as well as conditions that the real world imposes on the platform.

Foundation 3, discrete and continuous mathematics, highlights advanced math beyond calculus needed for CPS engineering. This reflects the fact that CPS deals with both continuous and discrete systems, and the knowledge on how to deal with that integration is critical.

Foundation 4, cross-cutting application of sensing, actuation, control, communication, and computing encompasses knowledge of control, signal processing, and embedded software design and implementation that one would expect to permeate all aspects of the curriculum

Foundation 5, stresses the need for modeling of heterogeneous and dynamic systems integrating control, computing, and communication with an emphasis on uncertainty and heterogeneity. Such work is especially challenging because physical and cyber modeling use different and often incompatible models. Focusing on the merging and interactions of models across the physical and cyber aspects of systems is necessary.

Foundation 6, CPS system development identifies the requirements for a life-cycle view of developing a CPS from initial requirements to certification to deployment. Concepts that transcend the entire life cycle include safety, resilience, security, and privacy.

SYSTEM CHARACTERISTICS

Building systems that operate with increased confidence in the presence of uncertainty and with acceptable levels of risk requires an understanding of how to address relevant design aspects (i.e., security, reliability, and dependability). Consider, for example, what it takes to design a city-scale autonomous transportation system that people can confidently use with minimal safety concerns. The committee also sees examples of gaps in today's deployed systems, such as the vulnerability to cyberattacks and poor interoperability. The following attributes and the associated design approaches and mindset are best introduced early in the CPS curriculum and infused throughout in CPS coursework and projects:

Security and privacy. All information technology-based systems are subject to cyberattacks. Many CPS are especially vulnerable either because they are located in open environments or can be communicated with wirelessly. Ensuring that those designing such systems are familiar with security and privacy risks and techniques for protecting them will be crucial.

Interoperability. Especially in large-scale CPS, systems will be composed of components from different vendors, and portions may be operated by different entities. Realizing the full promise of CPS will require interoperability among heterogeneous components and systems. Achieving interoperability requires knowledge of how to define and use common architectures, standardized interfaces, and data standards.

Reliability and dependability. Many CPS will be part of our daily lives, and their utility will require high reliability and dependability. New problems arise because many CPS devices have limited computational power, memory, and energy. The best systems are those designed from the start with reliability (and safety) in mind—not as something to be fixed during testing. CPS will also need to be robust to uncertainties that may be difficult to quantify in the design phase.

In order to make sure these uncertainties are addressed, they must be tracked and addressed during implementation stages.

Power and energy management. The compact size and autonomous operation of some CPS components make energy management a critical engineering design priority.

Safety. With the proliferation of CPS into daily lives, it becomes exceedingly important to ensure that actions taken on humans and the environment are safe and that the risks associated with these actions can be assessed and managed.

Stability and performance. The stability of CPS, which are dynamic and stochastic systems, involves such factors as the linearity or nonlinearity of the system, the bandwidth of the systems, sampling rate, the poles and zeroes of the system, the modeling of the noise and uncertainty affecting the system, and limitations of sensors and actuators such as noise corruption or saturation.

Human factors and usability. Human factors design, human-in-the-loop control, and understanding and accounting for the behavioral responses of humans are all important for many CPS applications. For instance, critical CPS are used to support the health care and well-being of the elderly.

These considerations are often essential in ensuring a system will operate with increased confidence in the presence of uncertainty and with acceptable levels of risk. The importance of improving education in these areas is highlighted by the prevalence of cyberattacks against CPS, poor usability, and lack of interoperability.

Most CPS will have to be developed with these system characteristics in mind. As a result, these concepts will need to be woven throughout a state-of-the-art CPS curriculum at all levels. The challenge in building software and hardware systems that have these properties is not unknown to the computer science and engineering domains. Exploring these challenges and learning how to determine if systems have these properties are essential to deploying better CPS.

1.10 CYBER-PHYSICAL SYSTEMS (CPS) IN THE REAL WORLD-

The term “Cyber Physical system” was initially coined by Ellen Gill in 2006. CPS is a category of embedded system. It is often called a Next Generation Computing System which uses smart computation techniques associated with physical world and computational units. The CPS can interact with the real-world systems by means of Computation, Communication and controls. The interaction of computational and physical units leads to advanced implementations of Internet of Things (IoT). IoT and CPS are designed to support real time applications which can manage many environmental datasets. In other words, CPS is a combination of digital controls and the physical environment.

2. INTRODUCTION

The Cyber Physical System consists of cyber components and physical components, so we call it as cyber physical system. CPS is based on an information processing computer system, which is embedded into a product, like a car, plane or other device. These computer systems are used to perform specific tasks.

For Example, in a car an embedded system would be the ABS (Anti-lock / Anti-Skid Braking System) to control break force. This computer system interacts with the physical environment by means of Sensors and Actuators. These embedded systems are no longer standalone, they share their data via communication networks such as the internet with cloud computing where data from many embedded systems can be collected and processed. Thereby creating a system of systems. Connected embedded systems can be controlled and decentralized by a computational unit. The collected data can be processed automatically or by Human Machine Interface (HMI).

IoT is a technology, in which devices are connected through the internet and enables the remote collection of real time information which can them be processed or shared with other devices.

CPS’s are powered by two types of computing system:

(i) Notebooks, Desktop servers and PCs. Computers at every desk to do business activities
(ii) Embedded Computing - Transformation of Industry and Invisible part of Environment.

The main characteristics of CPS are:

(i) Intelligence - Adaptive and Robustness
(ii) Network – Communication, Cooperation and Cloud solutions
(iii) Functionality

(iv) User friendly. The main features are as follows: CPS is said to be closely integrated with computation and physical processes, the software is embedded with physical systems and CPS networks use wireless sensor networks.

3. APPLICATIONS

The application of CPS have the potential to introduce significant changes in information intensive technology sectors such as manufacturing, water distribution systems, transportation, healthcare and smart buildings.

Manufacturing:

In manufacturing environment CPS's are used for self-monitoring the production operations and control. CPS improves manufacturing processes by sharing information between machines, supply chain, suppliers, business systems and customers. Smart manufacturing provides high visibility controls on the supply chain which results in improving the traceability and security of goods. The impact of IoT and CPS in manufacturing industry is significantly growing. Sensors are used to predict equipment wear and diagnose faults. The analytics reduces the maintenance cost and increases operation performance.

Manufacturing industries works under a five-level architecture.

Connection- Data is generated by machines, tools and the product
Conversion- Using algorithms it converts the data to information.
Cyber- Processes the information and creates additional value. Cyber level acts a hub (cloud) and performs complex operations. Cyber level runs on sophisticated manufacturing methods, runs deep learning algorithms to identify large data patterns. This level focuses on standalone systems which uses the data from the system to attain additional knowledge.
Cognition- Converts machine signals to information to compare the information with other outcomes. In this level the machine monitors and diagnoses its own failures and become aware of potential problems.
Configuration- a machine can track and detect failures early and sends information to the operation level. Machines can amend their operation depending on workloads or malfunctions.

These measures produce a system in which machines can defend themselves from difficulties by finding alternate solutions and preventing operation failures.

The 5c structure uses different levels of operations:

Component level: Contains virtual twins that exists in cyber space. The twin models the critical components of a machine. It captures the changes in the operations on the cloud. The system would gain self awareness by this mechanism.
Machine Level: Incorporates the information gathered in the component level which is combined with machine operations to create new modules for each machine. Similar Virtual twins are compared with other machines to quantify performance.
Fleet Level: Optimize production processes through the performance of machines and component status from component and machine levels. These level result in self configuring and self maintenance and has the benefit of maximizing the life span of all components, leading to increased production quality.
Enterprise Level: This level incorporates the outcome of previous levels to produce a high-performance production rate.

Water Distribution Systems:

Water Distribution systems are becoming increasingly automated. These systems consist of reservoirs, tanks, pumps, wells and pipes that deliver water to our taps. As well as devices to monitor activity such as sensors to detect the level of overflow of water from a tank or the pressure from the pipe. And programmable Logic Controls which can automatically open valves and supervisory controls and data acquisition systems that monitor controls all the devices in the network. While all these innovations allow the system to run more efficiently and reliably. They also expose the system to potential attacks on the software that controls it. If the hacker can remotely access the components of the CPS, they could do all sorts of damage ranging from stealing data, cutting of water supplies, damaging the equipment or even releasing chemicals used in processing into the system. Hackers can spy on the system with eavesdropping attacks or by initiating deception attacks.

It is difficult to detect the attacks on the system by human oversight and by machine detection algorithms. In order to overcome these attacks two types of tools are used. The first one is an 'Attack Model' the other is a 'Toolbox'. The Attack model describes the different way the hackers might compromise the system and the Toolbox runs on a MATLAB which is widely used engineering computing software. The Toolbox gathers the attack models and automatically runs on Epanet. An Epanet is an industry standardized software modeling tool which describes how water flows through the system. The Epanet utilizes the CPA toolbox to track the actual physical status of the system and the reported cyber status of the system which detects external changes introduced by the hackers.

Smart Greenhouse:

CPS play a vital role in the field of agriculture; it improves productivity and prevents starvation. The system focuses on an adaptive method with several parameters such as temperature, humidity, irrigation and amount of light. This responds to the parametric changes according to specific computer programs which are designed to ensure a better growth. Further it reports feedback continuously to the users to keep them informed about the condition of the greenhouse. Feedback can be managed easily by remote locations using network service. The design consist of sensors which act as a station sensor which includes temperature, humidity, soil moisture and light sensors and it adds other sensors like temperature and humidity control system in which the fan, sprinklers and other devices can be used for increasing and decreasing the temperature.

Benefits:

- It saves the farmers money, time and effort
- Provides better environment and increases in productivity
- The amount of water needed is controlled and supplied automatically

Health Care:

Most of medical systems use cyber physical systems, they use real time monitoring and remote sensing of physical conditions of the patients. This leads to improved treatments for disabled and elderly patients and limits patient hospitalization. In future these systems will be combined into a network closed loop system incorporating a human loop to improve the safety and workflows.

Transportation:

Vehicles can communicate with each other by sharing real time information such as traffic, locations and issues to prevent from accident and improve safety. Vehicles function will be executed in a distributrd manner by enhancing performance and emission reduction. For example, the branking system not only stops the car also it avoids a potential collision.

Buildings:

CPS enabled buildings are called "smart buildings". The function significantly improves energy efficiency and decreases energy consumption and greenhouse gas emissions. A network is used to sense the temperature, humidity and operate actuators (HVAC, fans, water heater) is embedded into the building to detect changes in the environment.

Claytronics:

Claytronics – a technology to create virtual reality with which human interaction is possible. IT combines nano scale robots and computer theory to make nanometer-scale systems called claytronic atoms / catoms. These catoms can interact with others to make 3D structures. The goal of claytroics is to create dynamic motion in three dimensional objects. Two types of algorithms are being used in Claytronics, shape sculpting and localization. The collective actuation and hierarchal planning require shape sculpting algorithms by which it converts the catoms into the desired structure and dimension. The localization algorithm enables the positioning of catoms in the ensemble.

1.11 NEXT GENERATION SENSORS

1.11.1 Handheld Molecular Contaminant Screener

HMCS (Handheld Molecular Contaminant Screener)- The user-friendly portable mass spectrometer that measures your sample within minutes.

Portable

No Sample preparation

User friendly

Block Chain- Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.

Tailored solutions for every industry

https://youtu.be/kizl8MJu9XI

1.12 COLLABORATIVE PLATFORM AND PRODUCT LIFECYCLE MANAGEMENT

What is a collaborative platform?

A collaborative platform is a virtual workspace where resources and tools are centralized with the aim of facilitating communication and personal interaction in corporate project work. This naturally means providing access to information, but also and importantly, encouraging collaboration in project tracking directly via the platform about:

- Project updates, monitoring and management;

- Document sharing (spreadsheets, presentations, text files, etc.);
- Exchanging information and communication about initiatives in progress.

The aim of a collaborative platform is to enable staff to work better together by simplifying their project monitoring tasks and delivering efficiency gains. Such a platform is an **innovative solution for businesses seeking productivity, financial savings and enhanced employee well-being**.

Different types of platform exist, depending on the type of project concerned. Some solutions will adapt themselves to all projects, while others require some customization. In any event, it is advisable to choose the solution that meets your main objectives in terms of collaboration:

- **Project portfolio management**;
- **Continuous improvement**;
- **Development of innovation**.

Product Lifecycle Management (PLM)

Introduction to Product Lifecycle Management

Product lifecycle management, sometimes "product life cycle management", represents an all-encompassing vision for **managing all data relating to the design, production, support and ultimate disposal of manufactured goods**.

PLM concepts were first introduced where safety and control have been extremely important, notably the aerospace, medical device, military and nuclear industries. These industries originated the discipline of configuration management (CM), which evolved into electronic data management systems (EDMS), which then further evolved to product data management (PDM).

Over the last ten years, manufacturers of instrumentation, industrial machinery, consumer electronics, packaged goods and other complex engineered products have discovered the benefits of PLM solutions and are adopting efficient PLM software in increasing numbers.

PLM solutions

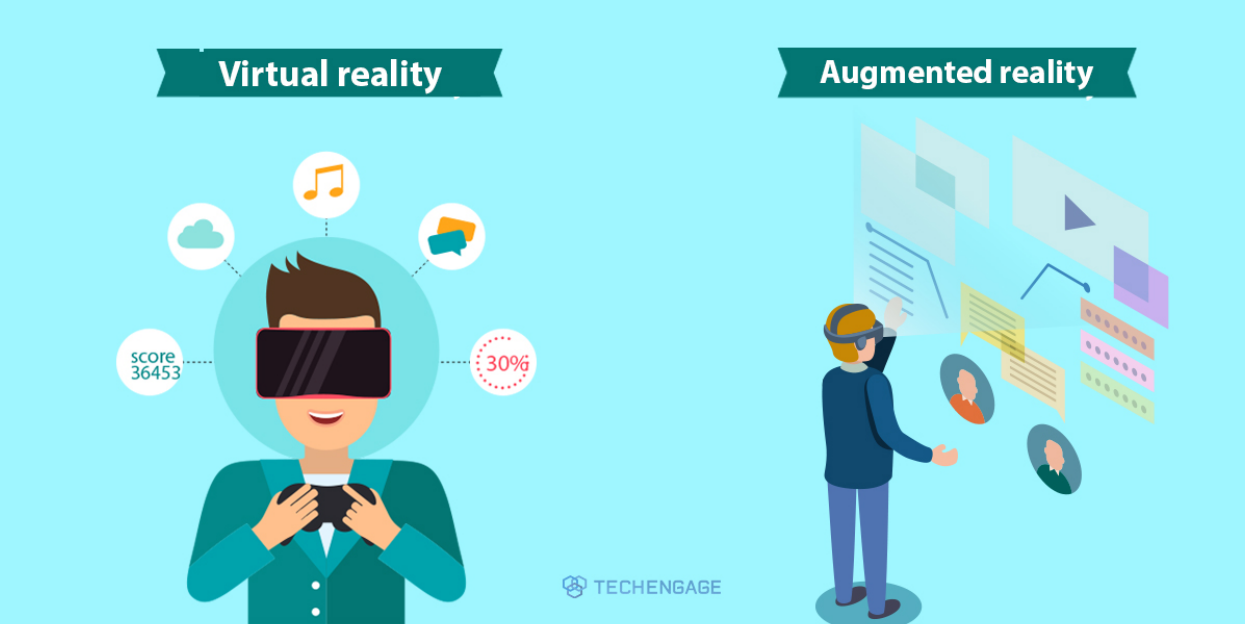
PLM can be thought of as both (a) a repository for all information that affects a product, and (b) a communication process between product stakeholders: principally marketing, engineering, manufacturing and field service. The PLM system is the first place where all product information from marketing and design comes together, and where it leaves in a form suitable for production and support.

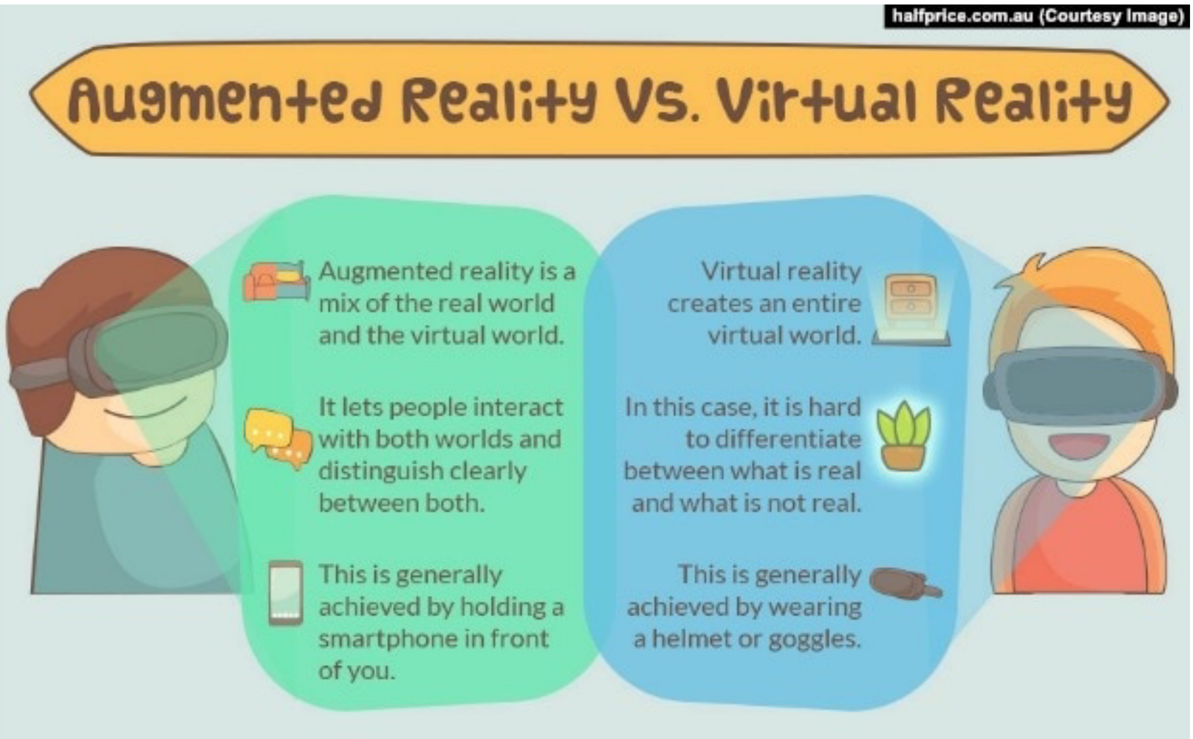
A few analysts use "PLM" as an umbrella term that includes engineering CAD (for "information authoring"). But product information creation tools include word processors; spreadsheet and graphics programs; requirements analysis and market assessment tools; field trouble reports; and even emails or other correspondence. In our view, a PLM tool focuses exclusively on managing data that covers the breadth of a product's lifecycle, without regard to how that data is developed.

The essential elements of PLM:

- Manages **design and process documents**
- Constructs and controls **bill of material** (product structure) records
- Offers an **electronic file repository**
- Includes built-in and custom **part and document metadata** ("attributes")
- Identifies **materials content for environmental compliance**
- Permits **item-focused task assignments**
- Enables **workflow and process management** for approving changes
- Controls **multi-user secured access**, including "electronic signature"
- Exports **data for downstream ERP systems**

1.13 AUGMENTED REALITY AND VIRTUAL REALITY





Augmented reality and virtual reality (commonly abbreviated as AR and VR respectively) are reality technologies that either enhance or replace a real-life environment with a simulated one. Augmented reality (AR) augments your surroundings by adding digital elements to a live view, often by using the camera on a smartphone. Virtual reality (VR) is a completely immersive experience that replaces a real-life environment with a simulated one.

In AR, a virtual environment is designed to coexist with the real environment, with the goal of being informative and providing additional data about the real world, which a user can access

without having to do a search. For example, industrial AR apps could offer instant troubleshooting information when a handset is aimed at a piece of failing equipment.
Virtual reality encompasses a complete environmental simulation that replaces the user's world with an entirely virtual world. Because these virtual environments are entirely fabricated, they are often designed to be larger than life. For example, VR could let a user box with a cartoon version of Mike Tyson in a virtual boxing ring.
While both virtual reality and augmented reality are designed to bring a simulated environment to the user, each concept is unique and involves different use cases. In addition to entertainment scenarios, augmented reality is also increasingly being used by businesses, because of its ability to generate informational overlays that add useful, real-world scenarios.

What Is AR?

Almost any person with a smartphone can get access to augmented reality, making it more efficient than VR as a branding and gaming tool. AR morphs the mundane, physical world into a colorful, visual one by projecting virtual pictures and characters through a phone's camera or video viewer. Augmented reality is merely adding to the user's real-life experience.

What Is VR?

Virtual reality takes these same components to another level by producing an entirely computer-generated simulation of an alternate world. These immersive simulations can create almost any visual or place imaginable for the player using special equipment such as computers, sensors, headsets, and gloves.

What's the Difference Between the Two?

The distinctions between VR and AR come down to the devices they require and the experience itself:

- AR uses a real-world setting while VR is completely virtual
- AR users can control their presence in the real world; VR users are controlled by the system
- VR requires a headset device, but AR can be accessed with a smartphone

AR enhances both the virtual and real world while VR only enhances a fictional reality

1.14 ARTIFICIAL INTELLIGENCE

WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence (AI) is a wide-ranging branch of computer science concerned with building smart machines capable of performing tasks that typically require human intelligence.

WHAT ARE THE FOUR TYPES OF ARTIFICIAL INTELLIGENCE?

- Reactive Machines
- Limited Memory
- Theory of Mind
- Self-Awareness

WHAT ARE EXAMPLES OF ARTIFICIAL INTELLIGENCE?

- Siri, Alexa and other smart assistants
- Self-driving cars
- Robo-advisors
- Conversational bots
- Email spam filters
- Netflix's recommendations

How Does Artificial Intelligence Work?

AI Approaches and Concepts

Less than a decade after breaking the Nazi encryption machine Enigma and helping the Allied Forces win World War II, mathematician Alan Turing changed history a second time with a simple question: "Can machines think?"

Turing's paper "Computing Machinery and Intelligence" (1950), and its subsequent Turing Test, established the fundamental goal and vision of artificial intelligence.

At its core, AI is the branch of computer science that aims to answer Turing's question in the affirmative. It is the endeavor to replicate or simulate human intelligence in machines.

The expansive goal of artificial intelligence has given rise to many questions and debates. So much so, that no singular definition of the field is universally accepted.

Can machines think? – Alan Turing, 1950

The major limitation in defining AI as simply "building machines that are intelligent" is that it doesn't actually explain *what artificial intelligence is? What makes a machine intelligent?* AI is an interdisciplinary science with multiple approaches, but advancements in machine learning and deep learning are creating a paradigm shift in virtually every sector of the tech industry.

In their groundbreaking textbook *Artificial Intelligence: A Modern Approach*, authors Stuart Russell and Peter Norvig approach the question by unifying their work around the theme of intelligent agents in machines. With this in mind, AI is "the study of agents that receive percepts from the environment and perform actions." (Russel and Norvig viii)

How Does Artificial Intelligence Work?

AI Approaches and Concepts

Less than a decade after breaking the Nazi encryption machine Enigma and helping the Allied Forces win World War II, mathematician Alan Turing changed history a second time with a simple question: "Can machines think?"

Turing's paper "Computing Machinery and Intelligence" (1950), and its subsequent Turing Test, established the fundamental goal and vision of artificial intelligence.

At its core, AI is the branch of computer science that aims to answer Turing's question in the affirmative. It is the endeavor to replicate or simulate human intelligence in machines.

The expansive goal of artificial intelligence has given rise to many questions and debates. So much so, that no singular definition of the field is universally accepted.

Can machines think? – Alan Turing, 1950

The major limitation in defining AI as simply "building machines that are intelligent" is that it doesn't actually explain *what artificial intelligence is? What makes a machine intelligent?* AI is an interdisciplinary science with multiple approaches, but advancements in machine learning and deep learning are creating a paradigm shift in virtually every sector of the tech industry.

In their groundbreaking textbook *Artificial Intelligence: A Modern Approach*, authors Stuart Russell and Peter Norvig approach the question by unifying their work around the theme of intelligent agents in machines. With this in mind, AI is "the study of agents that receive percepts from the environment and perform actions." (Russel and Norvig viii)

Norvig and Russell go on to explore four different approaches that have historically defined the field of AI:

1. **Thinking humanly**
2. **Thinking rationally**
3. **Acting humanly**
4. **Acting rationally**

The first two ideas concern thought processes and reasoning, while the others deal with behavior. Norvig and Russell focus particularly on rational agents that act to achieve the best outcome, noting "all the skills needed for the Turing Test also allow an agent to act rationally." (Russel and Norvig 4).

Patrick Winston, the Ford professor of artificial intelligence and computer science at MIT, defines AI as "algorithms enabled by constraints, exposed by representations that support models targeted at loops that tie thinking, perception and action together."
While these definitions may seem abstract to the average person, they help focus the field as an area of computer science and provide a blueprint for infusing machines and programs with machine learning and other subsets of artificial intelligence.

The Four Types of Artificial Intelligence

Reactive Machines
A reactive machine follows the most basic of AI principles and, as its name implies, is capable of only using its intelligence to perceive and react to the world in front of it. A reactive machine cannot store a memory and as a result cannot rely on past experiences to inform decision making in real-time.

Perceiving the world directly means that reactive machines are designed to complete only a limited number of specialized duties. Intentionally narrowing a reactive machine's worldview is not any sort of cost-cutting measure, however, and instead means that this type of AI will be more trustworthy and reliable — it will react the same way to the same stimuli every time.

A famous example of a reactive machine is **Deep Blue**, which was designed by IBM in the 1990's as a chess-playing supercomputer and defeated international grandmaster Gary

Kasparov in a game. Deep Blue was only capable of identifying the pieces on a chess board and knowing how each moves based on the rules of chess, acknowledging each piece's present position, and determining what the most logical move would be at that moment. The computer was not pursuing future potential moves by its opponent or trying to put its own pieces in better position. Every turn was viewed as its own reality, separate from any other movement that was made beforehand.

Another example of a game-playing reactive machine is Google's AlphaGo. AlphaGo is also incapable of evaluating future moves but relies on its own neural network to evaluate developments of the present game, giving it an edge over Deep Blue in a more complex game. AlphaGo also bested world-class competitors of the game, defeating champion Go player Lee Sedol in 2016.

Though limited in scope and not easily altered, reactive machine artificial intelligence can attain a level of complexity, and offers reliability when created to fulfill repeatable tasks.

Limited Memory

Limited memory artificial intelligence has the ability to store previous data and predictions when gathering information and weighing potential decisions — essentially looking into the past for clues on what may come next. Limited memory artificial intelligence is more complex and presents greater possibilities than reactive machines.

Limited memory AI is created when a team continuously trains a model in how to analyze and utilize new data or an AI environment is built so models can be automatically trained and renewed. When utilizing limited memory AI in machine learning, six steps must be followed: Training data must be created, the machine learning model must be created, the model must be able to make predictions, the model must be able to receive human or environmental feedback, that feedback must be stored as data, and these these steps must be reiterated as a cycle.

There are three major machine learning models that utilize limited memory artificial intelligence:

- **Reinforcement learning**, which learns to make better predictions through repeated trial-and-error.

- **Long Short Term Memory (LSTM)**, which utilizes past data to help predict the next item in a sequence. LTSMs view more recent information as most important when making predictions and discounts data from further in the past, though still utilizing it to form conclusions
- **Evolutionary Generative Adversarial Networks (E-GAN)**, which evolves over time, growing to explore slightly modified paths based off of previous experiences with every new decision. This model is constantly in pursuit of a better path and utilizes simulations and statistics, or chance, to predict outcomes throughout its evolutionary mutation cycle.

Theory of Mind

Theory of Mind is just that — theoretical. We have not yet achieved the technological and scientific capabilities necessary to reach this next level of artificial intelligence.

The concept is based on the psychological premise of understanding that other living things have thoughts and emotions that affect the behavior of one's self. In terms of AI machines, this would mean that AI could comprehend how humans, animals and other machines feel and make decisions through self-reflection and determination, and then will utilize that information to make decisions of their own. Essentially, machines would have to be able to grasp and process the concept of "mind," the fluctuations of emotions in decision making and a litany of other psychological concepts in real time, creating a two-way relationship between people and artificial intelligence.

Self-awareness

Once Theory of Mind can be established in artificial intelligence, sometime well into the future, the final step will be for AI to become self-aware. This kind of artificial intelligence possesses human-level consciousness and understands its own existence in the world, as well as the presence and emotional state of others. It would be able to understand what others may need based on not just what they communicate to them but how they communicate it.

Self-awareness in artificial intelligence relies both on human researchers understanding the premise of consciousness and then learning how to replicate that so it can be built into machines.

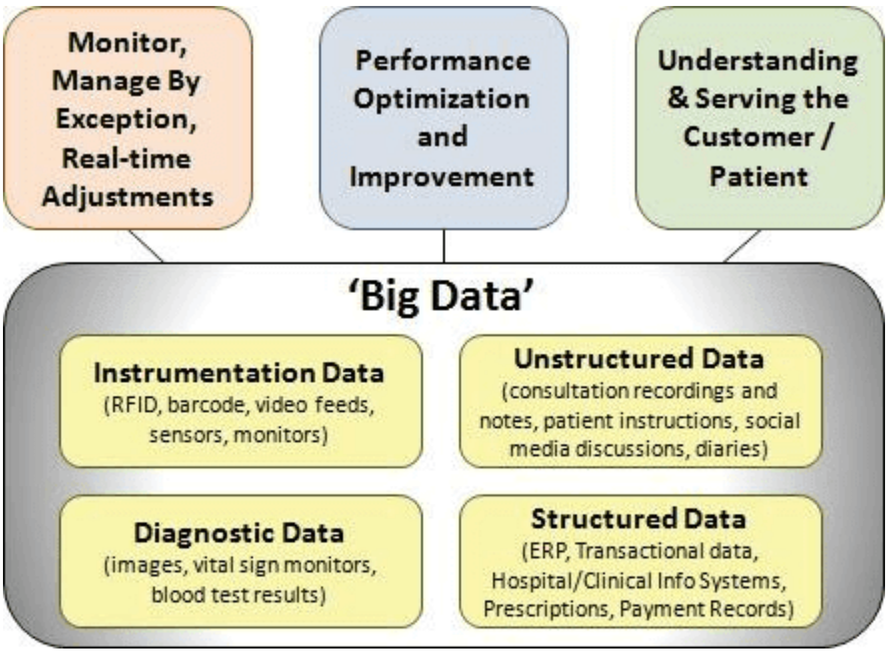
1.15 TRENDS OF INDUSTRIAL BIG DATA AND PREDICTIVE

The global big data market revenue is projected to hit the 103 billion US dollar mark by 2027. And, the current BI and analytics software market are valued at 16 billion USD globally.

Apart from the stats that speak a thousand words, big data, in association with AI, ML, and other technologies, is fueling what we call the Fourth Industrial Revolution. Big data analytics is one of the most powerful technology trends and is reshaping numerous business processes and operations across the world.

Rapidly expanding IoT networks, Data as a product, quantum computing, and data use for hyper-personalization there are many emerging trends in the big data segment.

Big data is also being used with AI, ML, and other innovative processing technologies to analyze, process, and parse the massive datasets in multiple sectors, such as Healthcare, eCommerce, Government Data, Public Infrastructure, Banking & FinTech, Security, Manufacturing, Natural Resources Management & Harnessing, etc.



Big Data in the Healthcare Sector

The latest studies reveal that in just 2 years, Big Data has spurred a change in the business perspective across the entire globe.

The following visual shows the major potential applications of Big Data, AI, and other technology landscapes:

With more than 2.5 quintillion bytes of data being generated daily. it is more than safe to assume that Big Data is gearing up for changing the way we think!

Predictive Analytics

Big data is empowering business organizations and data analytics stakeholders with its fundamental approach for quite a time now. It helps them to gain a competitive edge and accomplish their goals, such as better services, more sales, more customers, happier customers, and so on.

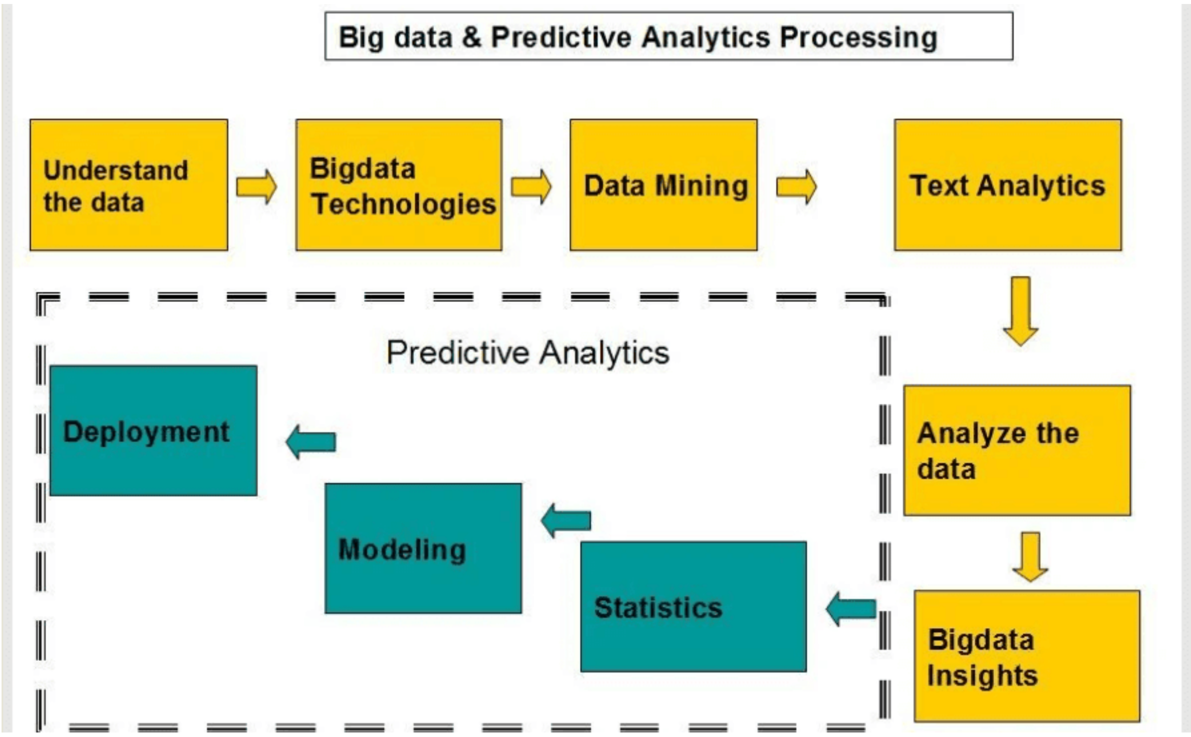
Business organizations use multiple tools to achieve these goals and predictive analysis is a common feature of these tools.

Predictive methods use historical events and modern data to uncover hidden trends and present actionable insights, such as:

- How many customers are going to leave your brand in the next 5 years with the current business approach?
- How many products can you sell in the coming quarter and what are the potential risks involved?

All in all, predictive analysis offers you a realistic and data-driven future prediction for various things. With advancements in Big Data, AI, ML, and other technologies, predictive analytics is all set to gain more power and offer more crucial insights.

So, you will be able to predict customer response, churn, purchase behavior and optimize your brand offerings, services, and business agendas accordingly.



Big Data and Predictive Analytics Processing

The visual shows how predictive analytics can identify the meaningful patterns of big data and generate future predictions to identify the value proposition of various options.

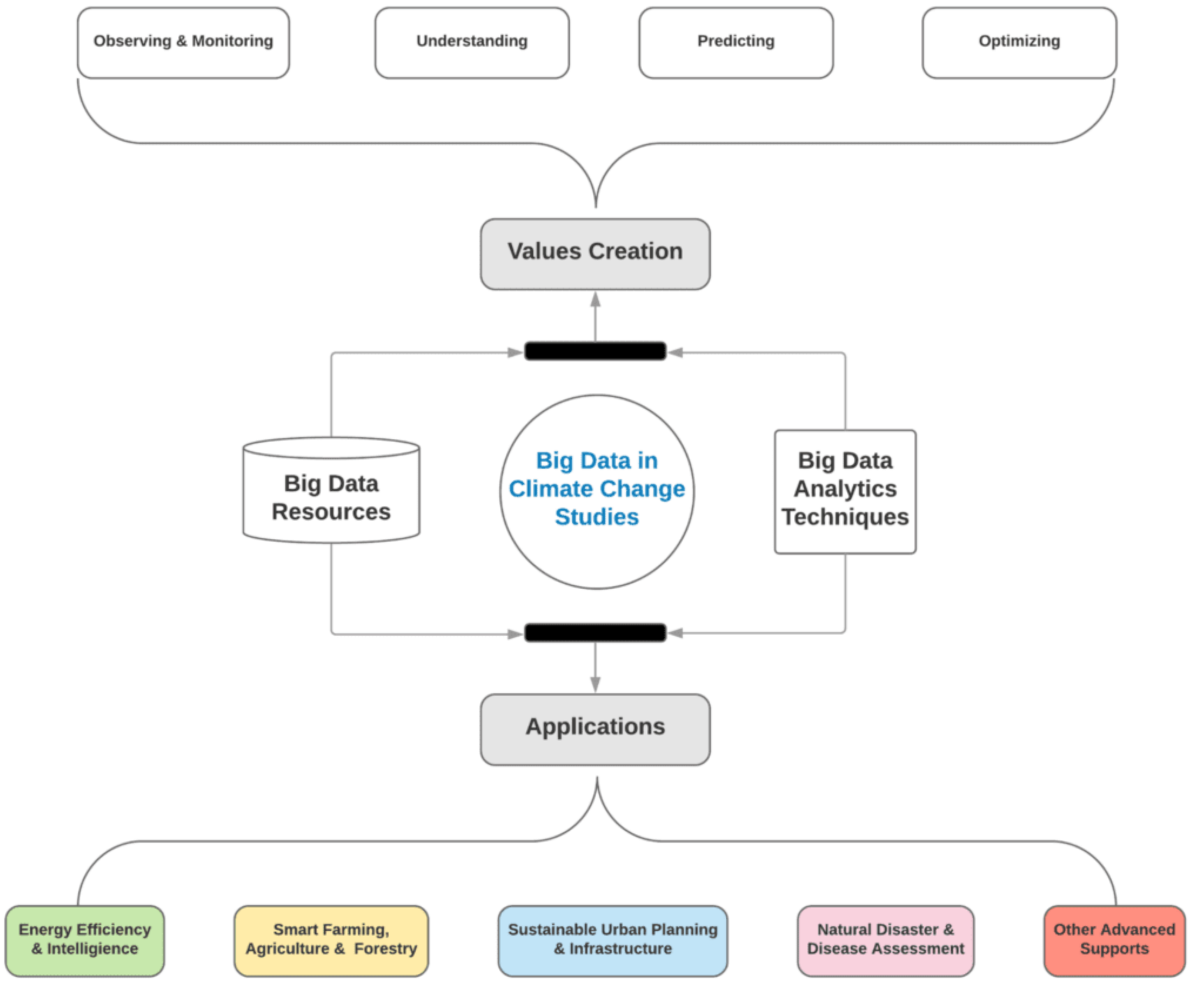
Climate Change Research

Climate change research comes under the umbrella term “X Analytics” that is coined by Gartner. “X” stands for a data variable for a wide range of structured and unstructured content, such as video analytics, text analytics, and audio analytics.

Leaders in the data analytics segment utilize X analytics to solve the toughest challenges to humanity, such as disease prevention, wildlife protection, and climate change.

Big Data, in unison with other technologies, such as artificial intelligence can comb through millions of research papers, news sources, clinical trials, and academic content pages to help climate researchers. The researchers can find new ways to contain the massive climate change, create containment plans for severe outcomes in red zones and identify the most vulnerable population pools via graph analytics, etc.

Take a look at the following visual that shows various ways big data can benefit climate change researchers:



Big Data in Climate Change Studies

Big Data analytics will also empower climate researchers to predict and plan for natural disasters and other such crises with its predictive models.

1.16ANALYTICS FOR SMART BUSINESS TRANSFORMATION.

What is analytic transformation in business?

Businesses that embrace analytics technology **transform their business models, and encounter new opportunities for customers, products, revenue streams, and services**. From sourcing materials and forecasting demand to the accounting and human resource activities, every aspect of the business can be with analytics.

2 Smart Analytics is **precisely analyzing in a smart and profitable manner all that volume of information**, which was impossible to do using traditional analysis methods. The goal behind Smart Analytics is to make the most out of all that information that is meaningless when served raw, but when correctly treated and analyzed, may imply a paramount change in the balance sheet of our company.

3 The smart analysis of Big Data is also **transforming the business world**. According to data presented by the CeBIT organization –the most important computer, information technology, telecommunications, software and services fair in the world– companies that use Big Data Analytics programs **are capable of making decisions five times faster** than those that do not work with Big Data. Moreover, 50% of the companies that do analyze Big Data ensure that this action lets them get a better grasp on consumer demand, boosting company growth.

Internet of Things (IoT): Smart Analytics

This concept refers to the **digital interconnection of everyday objects with the internet**, such as, for example, a refrigerator or a car. In this regard, according to the Gartner technology research company, by 2020 there will be approximately 20.4 billion “things” connected to the internet. The purpose of the “Internet of Things” is to **make our lives easier** in that it will be the objects themselves that make decisions and execute actions without the need for human intervention. One practical example could be a refrigerator connected to the internet that, once it has detected that milk has ran out, places an order to replenish it. We are faced with a reality in which “smart” machines will completely revolutionize the entire industry and market.

The “Internet of Things” will digitalize everything in the real world and integrate it to the internet. Therefore, the challenge lies in being able to collect and analyze the entire stream of information heading our way. Again, the concept of IoT data analytics reappears, which will be closely related to Big Data analysis. In this landscape, a real-time data analysis that enables us to make smart decisions instantaneously gains.