SYNAPSE

What is

?

By
Paul Ganichot
Heather Brundage

In this first post, we will define the Internet of Things, decompose its main components, summarize the IoT ecosystem, and demystify buzzwords such as Digital Twin, Digital Engineering, and Virtual Sensor.

Key Takeaway

The Internet of Things (IoT) is a complex system bridging the physical and digital worlds, generating large amounts of data.

This data is typically modeled as a Digital Twin.

The Internet of Things is a concept that has formed organically. The first connected device, a soda machine at Carnegie Mellon University in 1982, predates the internet as it was connected to ARPANET.
From an industrial perspective, the Supervisory Control and Data Acquisition (SCADA) control system was created in the 1970's to connect machines and automate their control; in other words, to make them smart. However, many argue that it took a coffee pot and a web cam connected to the internet in 1993 for the Internet of Things to be officially born.

Over the decades, the scope of the Internet of Things evolved to take advantage of technology advances and the definition has been updated and refined.

For this blog we define the Internet of Things (IoT) as a system of physical and digital components connected, and exchanging data, over the internet.

To dive deeper, the IEEE has a 70-page dissertation with a prudent title: "Towards a Definition of the Internet of Things (IoT)".

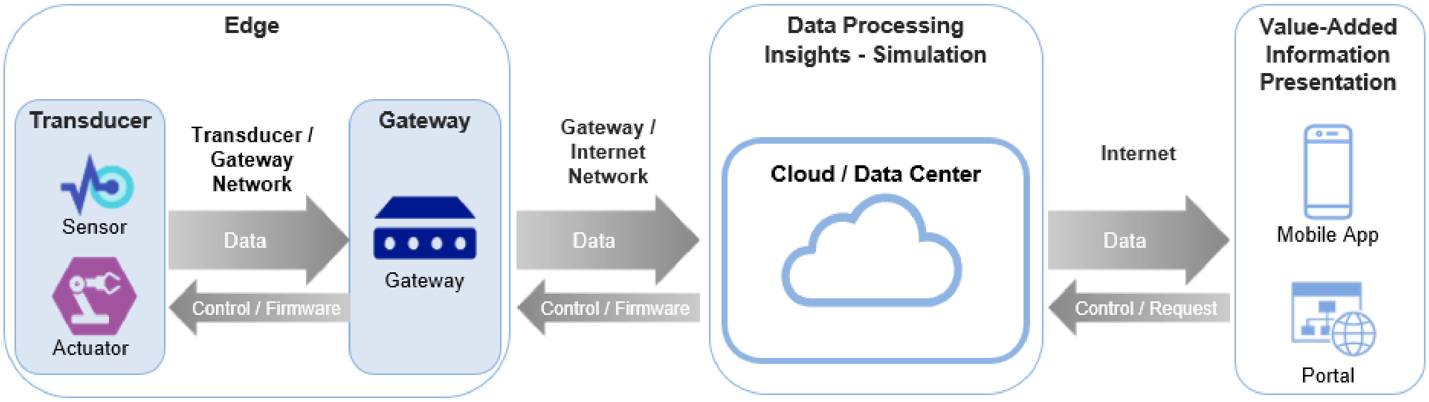
The Oxford English Dictionary offers the following definitions:

IoT: "The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data."

Internet: "A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication."

OVERVIEW OF AN IOT SOLUTION

The IoT overall architecture can be simplistically represented in tiers, with the corresponding network segments:



EDGE

The edge is the physical location where things connect with the networked, digital world. The Edge is where the IoT Device lives and where the physical and digital worlds interface.

TRANSDUCER, AKA AN "IOT DEVICE", A "THING":

A transducer provides a way to collect data (a sensor) or respond to data (an actuator); it converts variations in a physical quantity, such as pressure or brightness, into an electrical signal, or vice versa.

The resulting analog electrical signal may be converted to a digital signal by the transducer or by the gateway.

Transducers can be incredibly small, low powered and have limited functionality (such as a temperature monitor). They can also be large, high powered equipment that collects, processes, and transmits multiple types of data (such as an autonomous tractor).

A transducer and a gateway may be built within in a single device enclosure or may be separate devices connected through a network or electric wires; see the Topology section below for more details.
Sensors typically perform most of the data collection, but actuators may also report on their state.

Data elements collected by transducers may be referred to as: readings, tags, parameters, or measurements.

TRANSDUCER / GATEWAY NETWORK

Transducers and gateways can be connected through various technologies depending on the nature of the signal transmitted and the needs of the system:

- Digital signal: transducers that convert the analog electrical signal to digital signal transmit data to the gateway using a digital interface such as:
  - Wireless networks such as Bluetooth / BLE, Zigbee, LoRaWAN, Wi-Fi, …
  - Wired networks such as Ethernet, RS-485, RS-232, HART, …
- Analog signal: some transducers send the analog electrical signal to the gateway using electrical connections such as:
  - Wired electrical connections such as 4-20mA current loop, HART, 2-wire, embedded PCB, …

Note:
HART is a hybrid analog and digital protocol.

GATEWAY

A gateway provides a communication link between the edge and the cloud. It may also provide offline compute services and real-time control of devices in the field.Typically, it will support multiple communication protocols or networks.
For example an industrial IoT gateway may support the following communication protocols or networks:

- Transducer / Gateway: RS-485, GPIO pin-out, LoRaWAN, …
- Gateway / Internet: Wi-Fi, Ethernet, LTE-M, NB-IoT, 3G, 5G, …

GATEWAY / INTERNET NETWORK

Gateways have many options for connecting to the internet. The most common are via an ethernet cable, over Wi-Fi to a local router, or via a cellular network. Other possibilities include, but aren't limited to, Bluetooth, satellite, fiber, a low power wide area network (LPWAN), and/or acoustic modems.

DATA PROCESSING / INSIGHTS / SIMULATION

The bulk of data processing is often done on a cloud service provider or in a private data center capable of processing data streams from millions of devices and petabytes of data. This is also where most insights and knowledge are often generated, such as predictive maintenance and other machine learning & simulation models.

Note that some data processing and machine learning features may also take place on gateways with enough processing power, but the gateway is often limited to processing data streams related to the few sensors connecting to that gateway.

INTERNET / PRIVATE NETWORK

The value-added information output of the Data Processing / Insights / Simulation layer is transmitted to the users over the internet or over a corporate private network.

> Industrial IoT systems typically include a "**network of networks**" connecting transducers to gateways through different network technologies depending on the type of transducers and the physical layout of the edge site.

VALUE-ADDED INFORMATION PRESENTATION

The user experience and the presentation of the value-added information are critical components of a successful IoT solution as the volume of information can quickly become overwhelming. The presentation of the value-added information is often displayed in a mobile app, a website, or another screen, but can take many different forms and can include auditory or physical components.
A robust Value-Added Information Presentation layer typically includes dashboards designed for specific user roles, along with the corresponding insights visualizations and device management features.

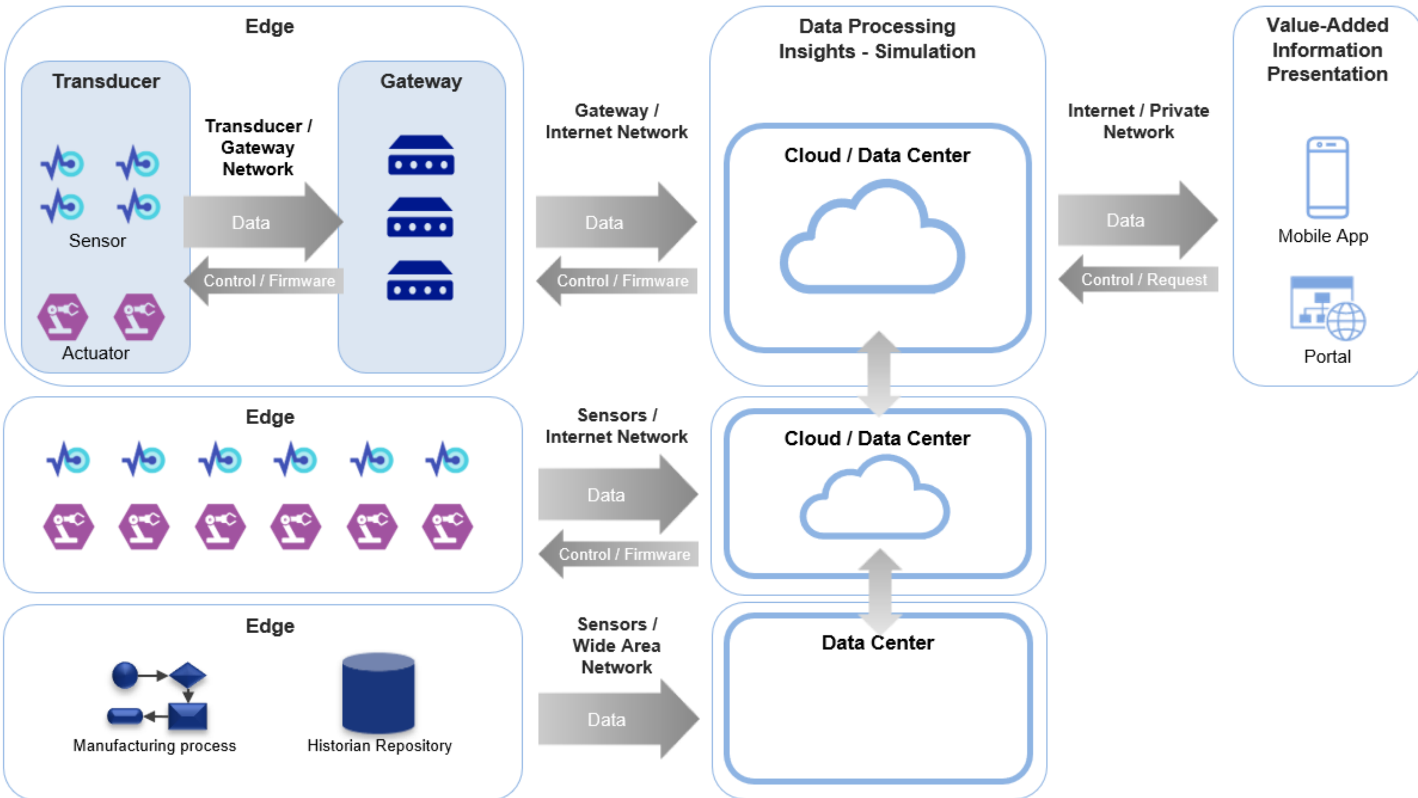
Examples of value-added information include:

- Virtual sensors: inferred parametric values computed from collected data of actual sensors to provide an estimate of the quantity of interest.
- Historical trends: aggregated visualization of many components, variance analysis, and correlation of collected data.
- Remaining Useful Life: predicted remaining lifespan of a physical components based on collected data for this component and many other similar components through an artificial intelligence forecasting model.
- Alerts: Triggered warnings when a threshold has been reached.

Note:
A systems perspective will be discussed in the "How to build an IoT solution" blog.

CONNECTED ECOSYSTEM TOPOLOGY

An actual IoT implementation can includes many different types of sensors and actuators, connecting to many gateways in many distant sites using different networks and communication protocols.
Some sensors and actuators may have a built-in communication capability, such as a cellular LTE module, and transmit their collected data directly to the Cloud / Data Center.
Contextual digital twins data sources such as a manufacturing process or a historian repository are also typical components. For example, the USGS is a typical historian repository leveraged for U.S. smart farming IoT solutions.



IOT ECOSYSTEM OVERVIEW

Because of the large number of technologies and architecture layers involved in IoT, there are many factors influencing a successful IoT journey.
Below is a summary decomposing these factors in four categories:

- Enablers
- Key Technologies
- Key Players
- Inhibitors

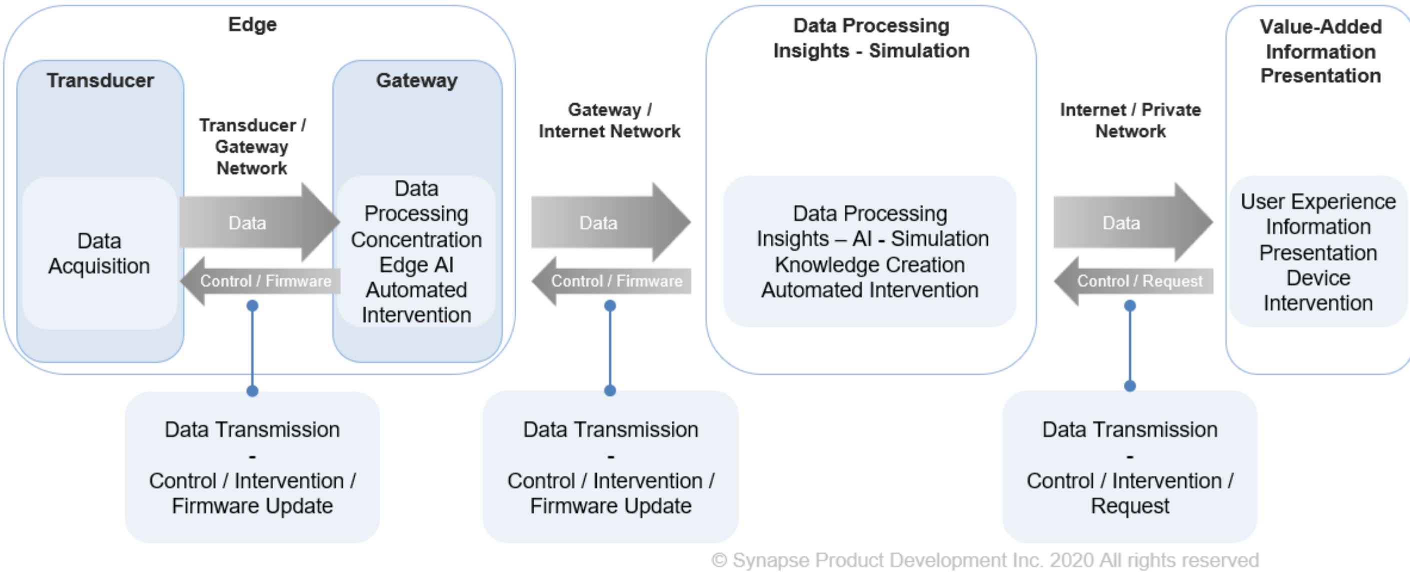
	Enablers	Key technologies	Key players	Inhibitors
Service	▪ Evolution from products to services ▪ Availability of scalable cloud services	▪ Cloud services ▪ IoT brokerage platforms	▪ Cloud service providers, e.g. Amazon Web Services ▪ IoT platforms e.g. Jasper Wireless	▪ Privacy and security concerns
Connectivity	▪ Network coverage ▪ Cellular standards ▪ Standards supporting new entrants ▪ Available spectrum	▪ Local area, e.g. Bluetooth, Wi-Fi, Thread ▪ Low power wide area (LPWA), e.g. LoRaWAN, Sigfox ▪ Cellular, e.g. 2G, 3G, 4G, NB-IoT	▪ Mobile network operators ▪ Ofcom ▪ Equipment developers and vendors	▪ Geographic coverage ▪ Cost ▪ Latency or capacity demands in some cases
Things	▪ Low cost sensors ▪ Improvements in battery technology	▪ Sensors specific to applications ▪ Actuators specific to applications ▪ Local processing, e.g. algorithms and artificial intelligence	▪ Device manufacturers ▪ Component and chipset manufacturers	▪ Security concerns ▪ Cost ▪ Scale
Market	**Payers** ▪ Consumers and end-users ▪ Companies ▪ Public sector		**Beneficiaries** ▪ Consumers and end-users ▪ Companies ▪ Public sector	
External factors	**Drivers** ▪ Cost savings ▪ Improvements in user experience ▪ Government policy and intervention		**Barriers** ▪ Appropriate business models ▪ Uncertainty of use cases ▪ Limited awareness	

Cambridge Consultants – Review of the Latest Development in the Internet of Things

IOT DATA FLOW

There are two main data flows in an IoT system:

- Data collected by the transducers flow from the edge to the main data processing layer and then to the user presentation layer.
- Device intervention and control flows from the users and/or from a data processing layer to the edge.



Note:
A data perspective will be discussed in the "How to build an IoT solution" blog.

DATA VOLUMES

The data collected by the transducers can quickly become voluminous.

Here are typical volume examples:

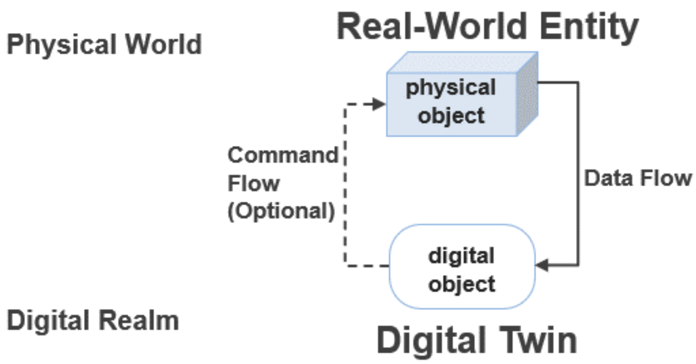
- Small industrial factory measuring efficiency of 4 machines through 2 sensors each at a 1 second frequency for 2 shifts 7 days a week: a 100 byte message payload generates 16 GB of data per year.
- Home automation for 1 million customers measuring a balance scale with 4 sensors each at 0.1 second frequency for 30 minutes per day every day: a 100 byte message payload generates 2,592 TB of data per year.
- Retail site with 20 object detection cameras taking pictures every 1 minute for 2 shifts 7 days a week: a 1.2 megabyte message payload generates 8 TB of data per year.

The data flowing from the users and/or data processing tier is comparatively very small, including the firmware updates. These firmware updates are larger files (typically ~ 100kB) but are infrequent (once or twice a year).

Organization of these large data volumes typically requires a cohesive data modeling approach.

THE DIGITAL TWIN MODEL

A digital twin is a digital representation of a real-world entity or system; it is used to model the data collected from the physical world at the edge into an organized digital construct closely resembling the physical object.



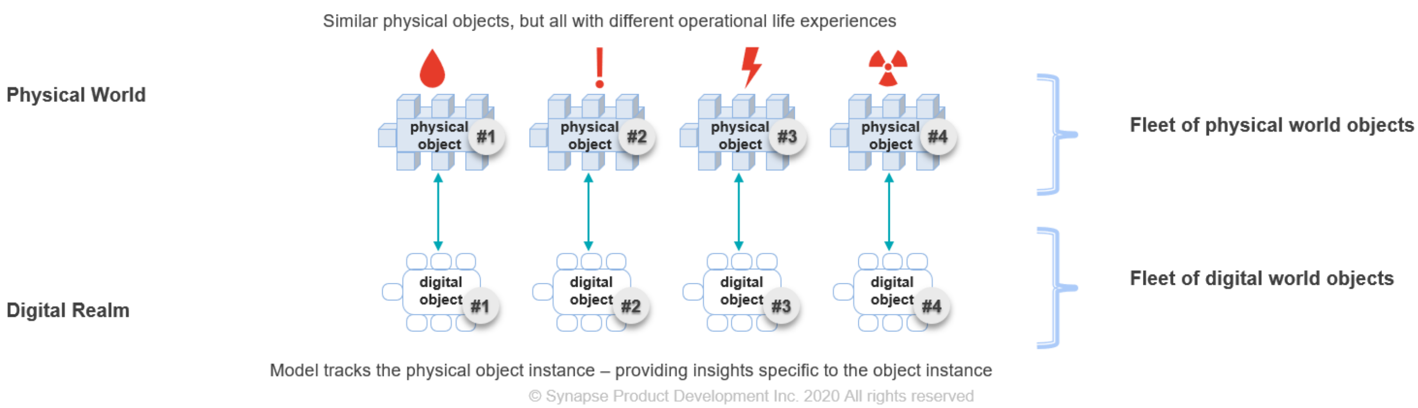
The Digital twin is a powerful concept and facility, with broad applicability such as twins of people, things, and systems.

The Digital Twin model enables the data to be processed into information, insights, and knowledge such as predictive maintenance and what-if simulations.

Achieving accurate and optimized benefits requires crucial, real-time data collection focused on answering key questions.

DIGITAL TWINS OF PHYSICAL OBJECTS

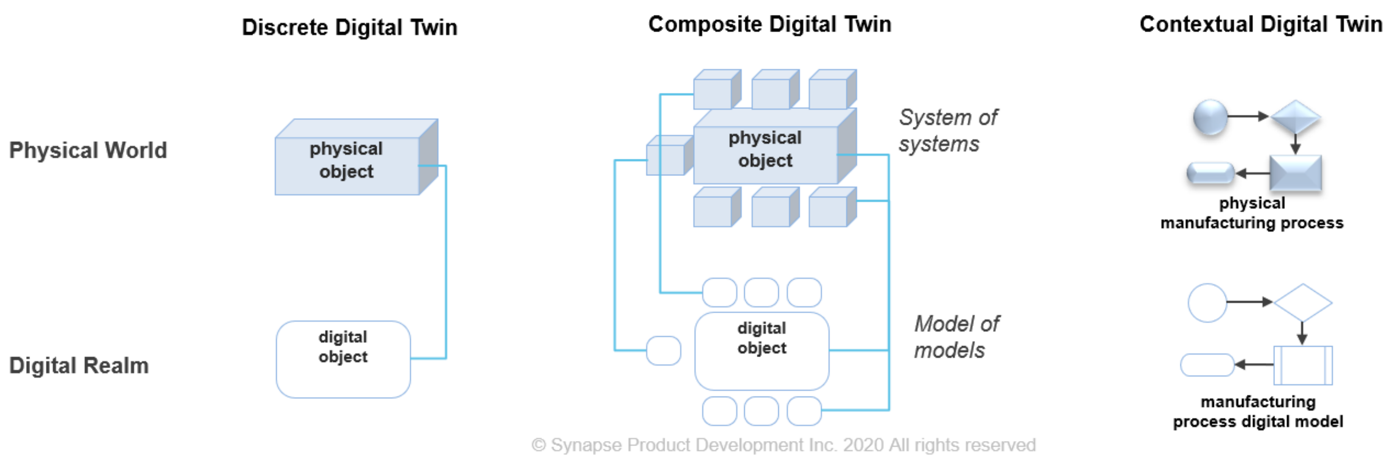
Digital twin instances model physical objects that evolve differently though different operational and environment conditions.



DIGITAL TWIN TYPES

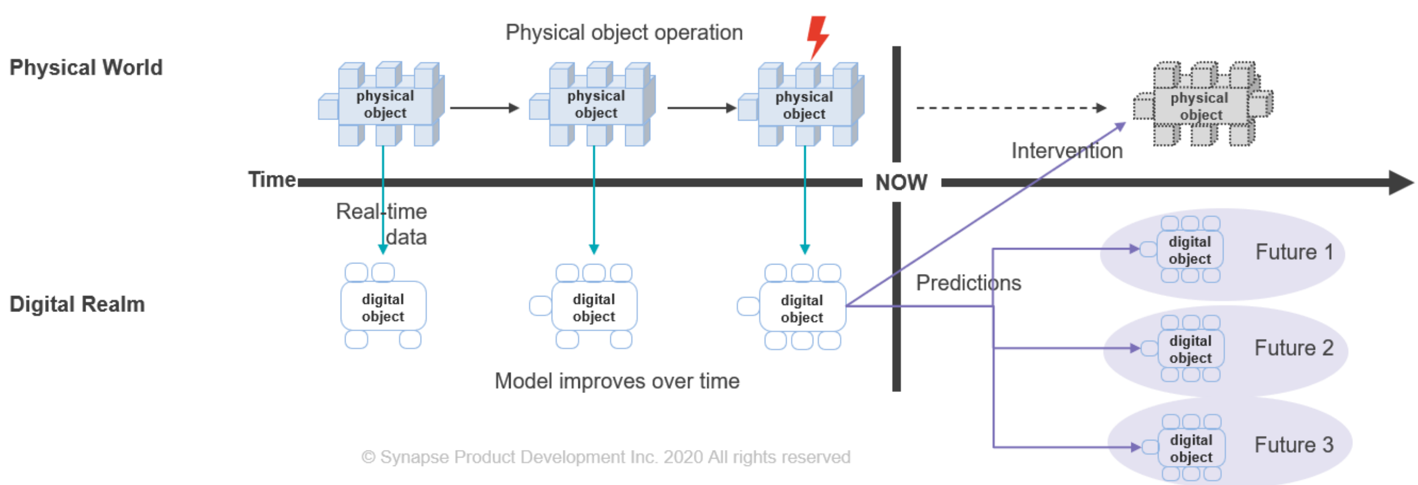
Digital Twins can be defined based on three categories:

- Discrete Digital Twin - a granular model representing an individual physical entity (e.g. propeller load sensor, propeller rotation sensor, individual frame load sensors, etc.)
- Composite Digital Twin - a system model representing multiple physical entities and their relationships; a Composite Digital Twin may comprise Discrete and Composite Digital Twins (e.g. propeller, complete frame, complete plane, etc.)
- Contextual Digital Twin – a model representing a process or contextual setting (e.g. process representation such as historic manufacturing steps characteristics, wind direction & speed, air temperature & humidity, other planes proximity etc.)



DIGITAL TWIN LIFECYCLE

The Digital Twin model can be built and enhanced gradually, with correlation and traceability between the different digital objects into systems.

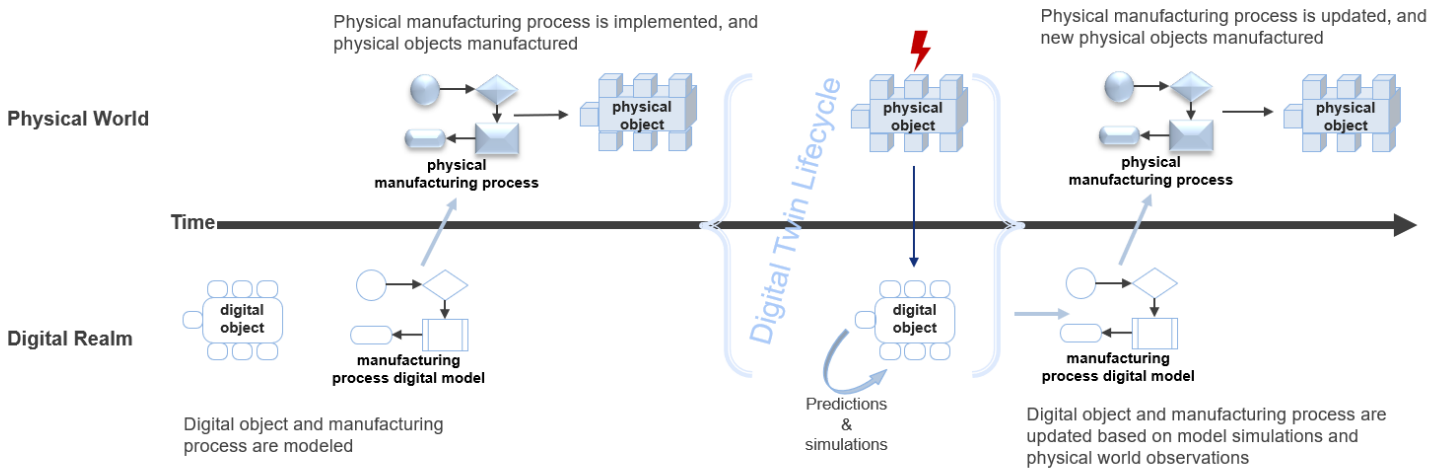


Data capture and streams can evolve over time to gradually tie into real-time operations/control where relevant by aligning to this model (e.g. start with batch data extraction after a flight, then process some operational data streams in the onboard Digital Twin, then add these streams to “real-time” transfers to centralized DT, etc.).

Machine learning for predictive maintenance can also be added gradually.

DIGITAL ENGINEERING

Digital Engineering (DE) is an integrated digital approach that uses authoritative sources of systems data and models as a continuum across disciplines to support lifecycle activities from concept through disposal.



Digital engineering describes a holistic approach to the design of a complex system: design using models/data instead of documents, integration of data across models, and the culture change across project teams to realize significant risk reduction on construction cost and schedule.

Now that we have framed “What is IoT”, we will explore in the next post why organizations purse IoT projects. We will show that IoT is about the “Information of Things”: the value of IoT follows the Pyramid of Knowledge, generating increasing value as data gathered from the IoT devices is processed into information and the resulting knowledge & insights.

SYNAPSE

Seattle
1511 6th Ave
Seattle, WA 98101
Ph: 206.381.0898

San Francisco
640 Bryant St
San Francisco, CA 94107
Ph: 415.361.5088

www.synapse.com