connected everything.
industrial systems in the digital age

Industrial Internet of Things

Applying IoT in the Industrial Context

Professor Duncan McFarlane
University of Cambridge

EPSRC
Engineering and Physical Sciences
Research Council

Contents

Summary

The brief report provides a positioning of developments in the area referred to as *Industrial Internet of Things (IIoT)* – loosely interpreting this as the *industrial developments* associated with the *Internet of Things (IoT).* IoT in turn describes the extension of the application of internet communications beyond computers and networked devices to also include the networking of everyday objects. In the context of industrial operations these objects are typically equipment, products and raw materials.

The Industrial Internet of Things is not a well-documented field at present and, as a consequence, this report begins with an overview of the Internet of Things as a whole in Section 1. In Section 2 those developments are specialised to consider issues specifically relevant to Industrial IoT. The report also positions Industrial IoT in the context of other industrial digitalisation initiatives currently receiving industrial and academic attention.
Finally, research directions in the areas of Sensors and Actuators, Communications, Infrastructure, Integration, Standardisation and Economics are proposed.

This report is not intended to be comprehensive and represents the author's view on the meaning and state of Industrial IoT.

A webinar which accompanies the report is located at:

http://www.youtube.com/watch?v=pj8ApxsymB4&feature=youtu.be

2. Internet of Things

2.1 Definition and interpretation of IoT

The Internet of Things (IoT) is one of the most widely used phrases in modern computing developments. Although often referred to as a technology, it is more accurately a platform for connecting objects (via sensing) so that data gathered about them might be used to analyse, interpret, decide and act on that data and other associated information.

According to TechTarget's Internet of Things Network Internet it is defined as follows:

*The **Internet of Things**, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. data.*[a]

Additional definitions by organisations such as IEEE and OASIS provide the same sense of IoT being a mechanism for connecting physical items to the internet:

A network of items—each embedded with sensors—which are connected to the Internet.[b]

A system where the Internet is connected to the physical world via ubiquitous sensors.[c]

In its simplest form, IoT is generally understood to comprise three key component levels (see a recent IEEE IoT paper[d], GS1s Internet of Things Report[e] and also the 2015 IEEE Report on Definitions of IoT[f] and the references therein):

1. *Edge functionality* – sensors (and actuators) connected to physical objects and machines.
2. *Data Gateways* – mechanisms for receiving sensed data from edge devices and transmitting to edge devices. Also capable of transmitting and receiving information from networked servers.
3. *Data Management & Analysis* – (cloud) server based collection, linking, analysis and use of data.

[a] Tech Target's Internet of Things Network, 2018 https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT
[b] IEEE, Special Report: *The Internet of Things*, 2014 http://theinstitute.ieee.org/static/special-report-the-internet-of-things
[c] OASIS, *Open Protocols*, 2014
[d] Chen, S., Xu, H., Liu,D., Hu, B. and Wang, H. *A vision of IoT: Applications, Challenges and Opportunities with China Perspective*, IEEE Internet of Things Journal, **1**, 349ff, 2014
[e] Barthel, H. et al, GS1 and the Internet of Things, Release 1.0, 2016
[f] Minerva, R., Biru, A., and Rotondi, D. IEEE Report, Towards a definition of the Internet of Things (IoT), Revision 1, 2015

Connecting these levels are the necessary communication systems. Edge to Gateway communications are supported by a myriad of wired and wireless communication methods (see Section 2.3).

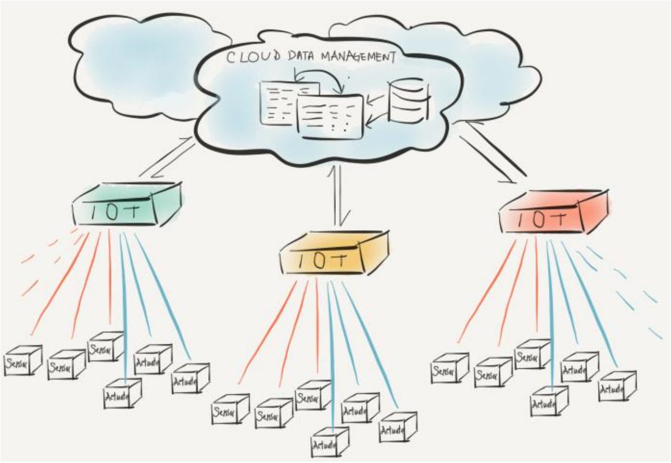


Figure 1: Conceptual of Schematic IoT

There are some common attributes of IoT as well as some misconceptions. These are summarised in **Table 1**.

IoT	Not IoT
• Enabling infrastructure • A means for connecting objects to other objects of machines • Extension of Internet (to include objects) • Enabling sensing, decisions and actions involving everyday objects	• An application or a service • A new separate network of objects • Just about getting object data from sensors • Mainly about big data • Mainly about data base coordination

Table 1: IoT Attributes

2.2 Background to IoT

The phrase Internet of Things is attributed to Proctor and Gamble Marketing Director Kevin Ashton[g], who in 1999 was working with P&G to link their enterprise computing systems to an automated form of product data collection based around RFID (Radio Frequency Identification). Ashton noted that a major limitation of computing, at the time, was that all data needed to be collected manually.

At the time, products such as RFID were used to enable remote data sensing. Auto ID Center[h] developed a new radical approach to very low cost RFID. Rather than house product data (expensively) in the memory on the RFID tag itself, the tag memory was simply provided with an identification number which when read would provide a link to further product data being (cheaply) stored on networked servers. As a result a commercial product following such a process would thus be linked to its data via an internet connection, further reinforcing the notion of an *internet of things*.

2.3 Vision

Although many of the commercial partners in this programme were simply seeking a like for like replacement for barcodes (albeit with better reading distances, rates and fewer line of sight constraints) the vision that evolved around these developments was rather more ambitious. In 1999 the MIT lab was activity seeking to use this RFID model to enable, for example, food products to communicate interactively with cooking equipment (see **Figure 2**).

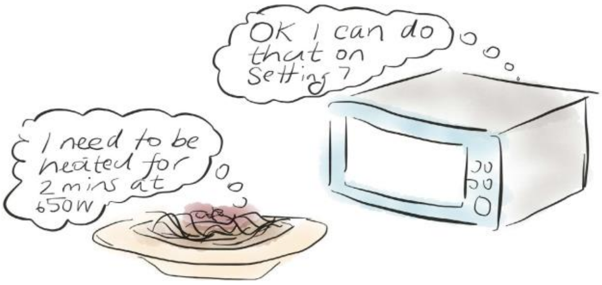

OK I can do that on Setting 7
I need to be heated for 2 mins at 650W

Figure 2: Food product interacting with equipment (Reworking of Auto ID Center graphic, 2000)

[g] Ashton provides an explanation of this in Ashton, K. *That Internet of Things Thing,* RFID Journal, June, 2009

[h] Auto ID Center ran a research programme examining electronic alternatives to the Bar Code, initiated at MIT in 1999, involving 100+ companies, University of Cambridge and Adelaide University and later University of St Gallen, Keio University, Fudan University and KAIST.

This notion of products being equipped with an ability to interact was formalised in 2002 with the introduction of a specification for an intelligent product[i].

An intelligent product is one which:

1. *Possesses a unique identity*
2. *Is capable of communicating effectively with its environment*
3. *Can retain or store data about itself*
4. *Deploys a language to display its features, production requirements etc.*
5. *Is capable of participating in or making decisions relevant to its own destiny*

2.4 IoT Functionality

Referring to **Figure 1** we make the following comments about some aspects of IoT operations.

1. *Edge – Gateway communications:* The underlying assumption is that many such communications will be wireless in nature, requiring some form of transmission/reception capabilities at both edge (device, sensor, actuator) and network gateway. The nature of the communication itself will depend on several factors but range and data rates will be significant factors in selecting a particular communications mechanism. This is illustrated in **Figure 3** and it can be seen that there are a vast range of communication options ranging from the high data rates over low range of Wifi 802.11 to low data rates and very high range [10 km] associated with the low power, wide area network approaches being generally proposed by LoRa / LoRaWAN[j] (open) and Sigfox[k] (proprietary), and for specific applications, like Texas Instrument's WMBus[l] for smart metering data collection.

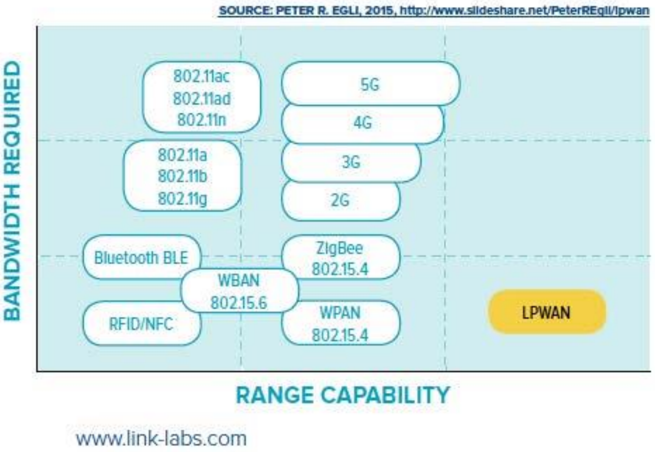


Figure 3: Different IoT Communications Approaches[m]

2. *Gateways:* Many devices can perform the functionality required from a gateway as described in **Figure 1** ranging from network capable RFID readers, to mobile communication masts. LPWAN gateways are most commonly referred to as IoT gateways which is accurate but it should be noted that these represent a small subsection of potential IoT traffic.

3. *(Cloud) Servers:* Because of the distributed nature of the data sources, servers supporting data management and analysis functions are typically cloud based. Some of the key functions required to support data management for IoT based sensors and devices are outlined in **Figure 4**. Importantly, it is noted that data analytics is just one of a number of functionalities required to support IoT data. Further information on IoT data management support can be found IEEEs 2015 report[f].

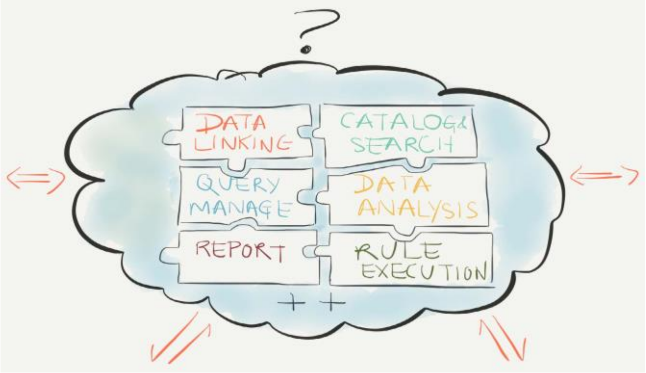


Figure 4: IoT Related Data Management Support

[i] Wong, C. Y., McFarlane, D., Zaharudin, A. A. and Agarwal, V. (2002). *The intelligent product driven supply chain.* Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, **4**, 393-398, 2002

[j] *A technical review of LoRa ® and LoRaWAN ™*, 2015

[k] See https://www.sigfox.com/

[l] See https://www.ti.com/tool/WMBUS

[m] Source: 2016 https://www.link-labs.com

2.5 Links to Internet

The internet was originally intended as a mechanism for allowing computers in different locations to communicate in order to allow for simple applications such as file transfers, electronic mail etc. Although viewed as a system it is more accurately a collection of communication devices and media combined in a standardised formation. It is supported by a set of standards which allow for the specification of communication media, protocols, data transport. In the 1990s the internet was increasingly used to also connect mobile devices and increasingly powered industrial equipment was also accessible via internet communications (see **Figure 5**). In the 2000s, the notion of inanimate (non-powered) objects also becoming part of the internet was introduced. The main challenge was that these items could not directly form a network connection, so the use of automated identification technologies (RFID, Bluetooth, bar code, QR code) provided a proxy connection – typically via some form of networked reading device. Further, in an industrial context, the Industrial Internet Consortium[n] has expended significant efforts establishing requirements for industrial internet applicability and then also considering how Internet of Things fits into this context[o].

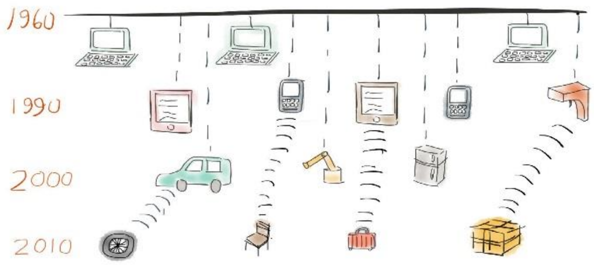


Figure 5: Extension of Internet: Mobile Devices, Equipment and Objects

2.6 Uses of IoT

In some ways, any solution for connecting sensed data to a data base could be termed an *IoT-solution,* but in this section we differentiate between ad hoc solutions for object sensing, tracking, actuation that might be developed for a particular application, probably within one location, and those for which systematic IoT based architectures have been explicitly used. Such applications are typically characterised by:

1. Applications requiring multi-organisation [object] sensed-data sharing

2. High variety & wide distribution of sensors / sensed data / data sources emerging

3. Cloud [internet] based application software is already in use for managing items in a particular domain (e.g. homes, offices)

4. Environments having little or no legacy data collection and management infrastructure.

To these characteristics, we add – predominantly for future applications:

5. Applications involving personalisation / customisation of products / orders / items [‘smarter things’]

Noting these characteristics, it is no surprise that cities, homes and office environments are early adopters of organised IoT sensed data management infrastructures (see **Figure 6**).

[n] Industrial Internet Consortium, http://www.iiconsortium.org/

[o] Industrial Internet Consortium, The Industrial Internet of Things Volume G5: Connectivity Framework, 2017 IIC:PUB:G5:V1.0:PB:20170228.

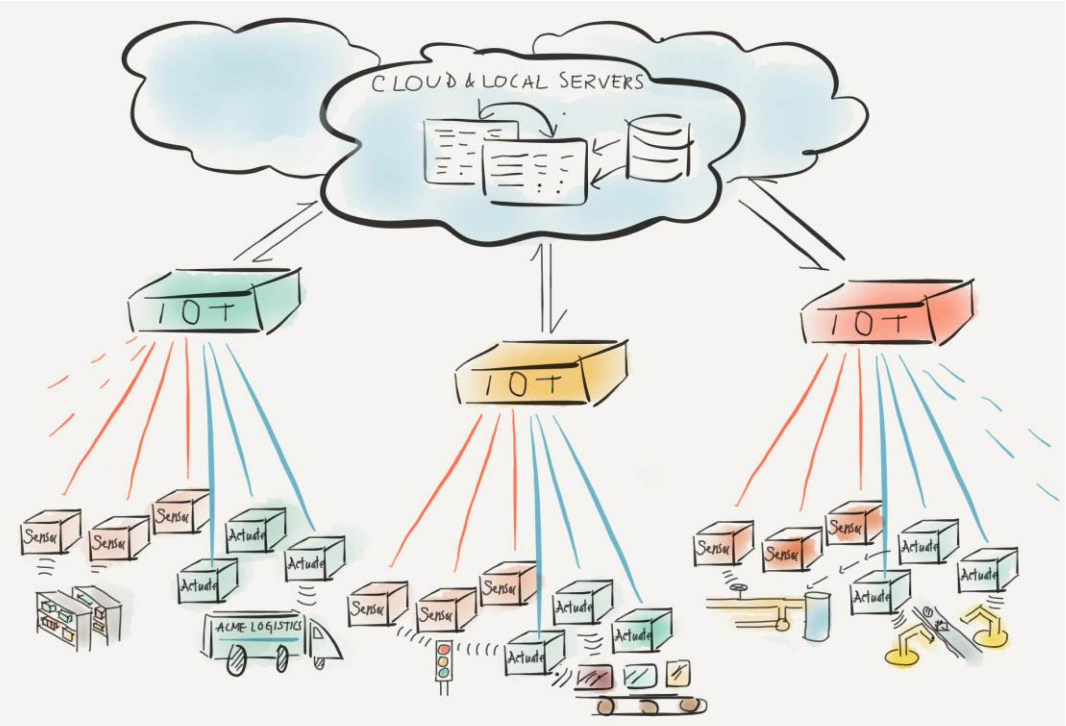
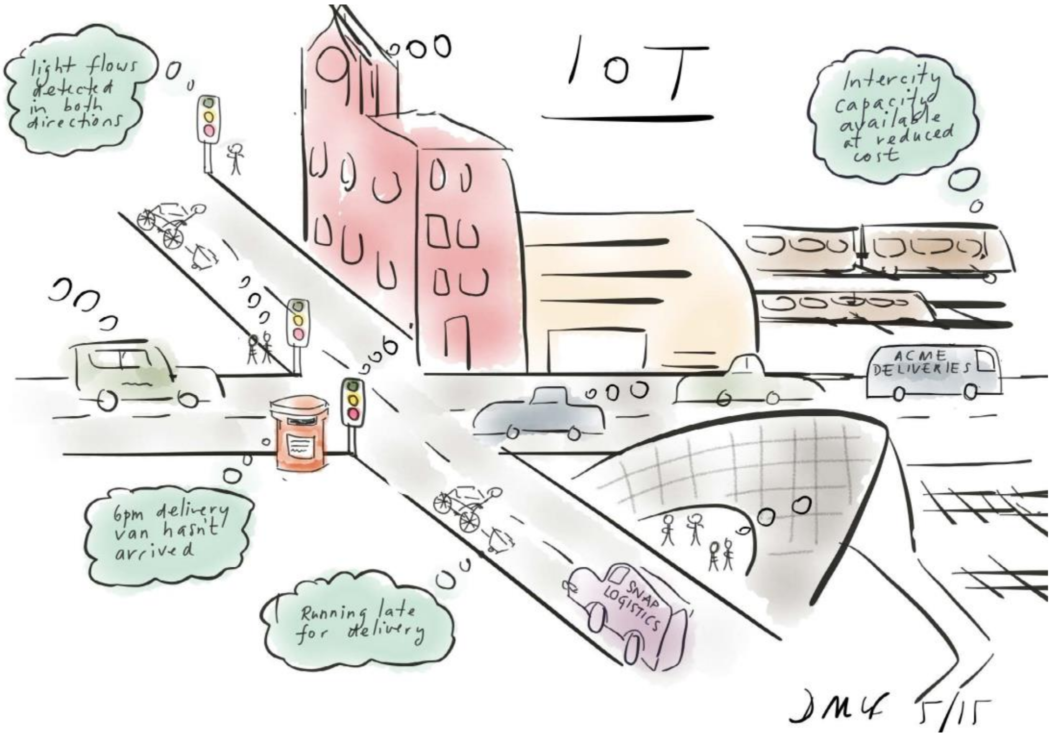


Figure 6: City based IoT Applications



light flows detected in both directions
IoT
Intercity capacity available at reduced cost
ACME DELIVERIES
6pm delivery van hasn't arrived
Running late for delivery
SNAP LOGISTICS
JMG 5/15

Figure 7: Industrial IoT Schematic

3. Industrial IoT

Given that in this report *Industrial Internet of Things (IIoT)* is loosely interpreted as the industrial application developments associated with the *Internet of Things (IoT)* the first part of the report has necessarily reviewed these developments. In this second part we interpret IoT in an industrial context, position it against other industrial digital systems paradigms and identify challenges for research and development.

3.1 Definition of Industrial IoT

Following the comments above, the definitions to be used here simply relate to the industrial use of IoT.

The term industrial Internet of things (IIoT) is often encountered in the manufacturing industries, referring to the industrial subset of the IoT [a]

Although in the context of this report we will use the rather more descriptive working definition:

The application of Internet of Things developments to (create value for) industrial processes, supply chains, products and services.

This is because it explicitly includes the role of products and services within its scope, as well as industrial processes and operations.

Following the general IoT schematic in **Figure 1**, we note that in the specific context of industrial applications, the edge objects that would be expected to be connected within IoT infrastructure consist primarily of products / parts / materials being transformed or transported and resources / machines / equipment used in the transform or transport processes (see **Figure 7**).

3.2 Uses of Industrial IoT

In this section, two specific benefit areas of IoT in an industrial context are raised. These relate to areas of sensing that are not traditionally part of the factory information environment and are hence not typically integrated into production or asset management considerations. In a later section, the differences between existing industrial IT systems and the options that IoT can offer will be discussed.

(i) Collecting Non-Production Data to Improve Industrial Operations: Industrial operations are extremely efficient at sensing production data to ensure best performance but generally less efficient at integrating data from maintenance, quality control and raw material supplies into considering production planning, scheduling and control issues. Part of the reason is the difficulty of integrating such data into the factory information & control environment. IoT can potentially help address this challenge by making this data accessible – even if it originates from 3rd party data suppliers. Conversely the use of production data for non-production needs (maintenance, quality control etc.) can also be enabled by some of the evolving Industrial IoT offerings. **Figure 8** illustrates different "layers" of manufacturing data: core production data, peripheral production data, factory wide data, supply chain data and ecosystem data. There is very little interconnection currently between these levels and this is partly because of the different information systems used.

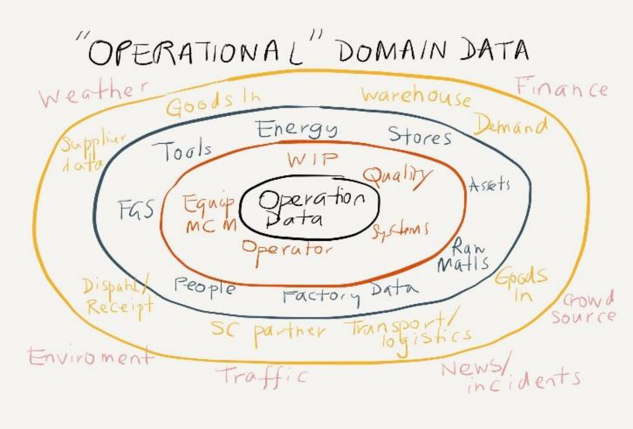


Figure 8: Layers of manufacturing related sensed data

(ii) Collecting Product related Data to Improve Product Life Cycle Performance: A second severe limitation of today's sensed data provision relates to product data and product-related process data as a product moves throughout its life cycle. Fragmented information relating to an industrial product lies in databases of suppliers, manufacturers, distributers, retailers and service providers etc. The work of the Auto ID Centre, EPC Global, GS1 and others over the last 15 years has been to create standards for the exchange of product data across multiple organisations. An industrial IoT framework in which product data could be seamlessly gathered and linked to a physical entity as it moves through its life cycle would address many of today's product life cycle management challenges. It might even enable

self-managing products, as illustrated in **Figure 9**.

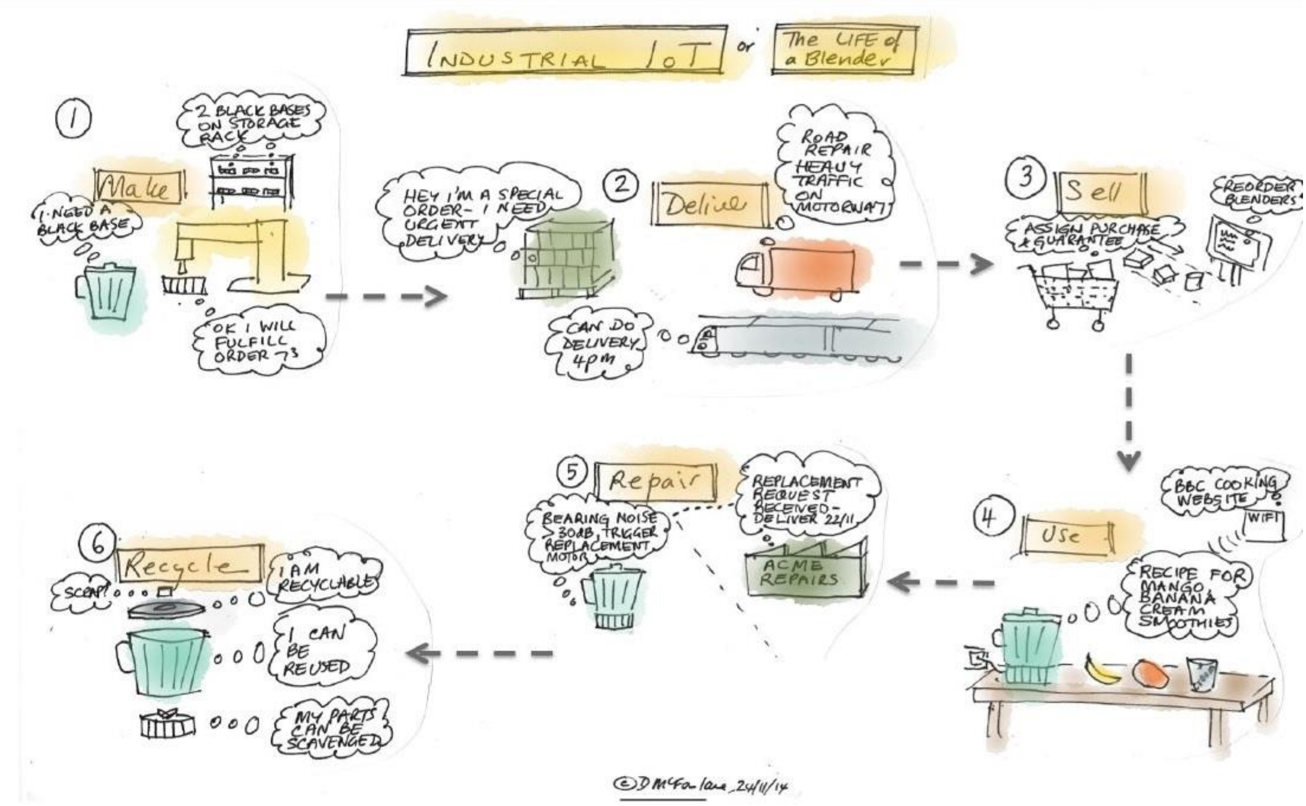

INDUSTRIAL IoT
or
The LIFE of a Blender
1
Make
2 BLACK BASES ON STORAGE RACK
I NEED A BLACK BASE
OK I WILL FULFILL ORDER 73
HEY I'M A SPECIAL ORDER - I NEED URGENT DELIVERY
2
Delive
ROAD REPAIR HEAVY TRAFFIC ON MOTORWAY
CAN DO DELIVERY 4pm
3
Sell
REORDER BLENDERS
ASSIGN PURCHASE & GUARANTEE
4
Use
BBC COOKING WEBSITE
WIFI
RECIPE FOR MANGO BANANA CREAM SMOOTHIES
5
Repair
BEARING NOISE >30dB, TRIGGER REPLACEMENT MOTOR
REPLACEMENT REQUEST RECEIVED - DELIVER 22/11
ACME REPAIRS
6
Recycle
SCRAP!
I AM RECYCLABLE
I CAN BE REUSED
MY PARTS CAN BE SCAVENGED
©D McFarlane 24/11/14

Figure 9: Industrial IoT supporting product life cycles

There is at this stage only a very limited, superficial literature on the deployment of IoT in an industrial context and even that coverage is cursory. It is extremely difficult to determine where reported applications have in fact benefited from specific IoT developments and where the reporting is simply that of a sensor application within an industrial context. Ignoring this distinction for the moment, applications that report the deployment of Industrial IoT solutions typically cover one of the following themes:

- *equipment monitoring* – gas turbines & construction equipment[p], trains[o], trucks[q]
- *maintenance* – aircraft[o], wind turbines[r], elevators[s]
- *quality control* – beverages[o]
- *energy management* – manufacturing[t]
- *productivity* – logistics[o], machine tools[o], oilfield production[p]
- *safety* – rail transport[o]

To summarise, the areas where Industrial IoT might provide the best immediate impact are applications in:

- Integrating data from suppliers, logistics providers, customers
- Introducing data from new technology, peripherals, tools, equipment
- Distributed production requiring addition of new data sources, locations, owners
- Sensors on board raw materials, parts, products, orders passing through organisations

3.3 Links to existing Industrial IT

As mentioned above, one of the challenges in articulating the impact IoT can make in the industrial space is to be able to differentiate between existing facilities for linking physical activities to computing via sensing and actuation and those additional capabilities that IoT developments can provide. This is noted for example in an IoT Report by the Digital Catapult[u]. Conventional industrial IT systems – e.g. those based around the so called Computer Integrated Modelling (CIM) principles[v] already allowed for standard data connections between production sensors and devices and data management computers (see **Figure 10**a) but IoT gateways integrated into the factory IT environment[w] would allow for a simple integration of production and non-production data (see **Figure 10**b) and potentially also allow for third party data from beyond the factory boundary (**Figure 10**c) to also be included. Conversely, such extensions will also allow for data from the production environment to be made available for uses elsewhere, for example, making production monitoring data from particular equipment available to the machine supplier or manufacturer or product quality data available to the end customer.

[p] Magee, T. *Seven industrial Internet of Things examples: IoT in heavy industry*, Computerworld, March 2016 https://www.computerworlduk.com/galleries/it-business/industrial-internet-of-things-examples-iot-in-heavy-industry-3636962/

[q] Bolen, A. *Internet of Things examples from 3 industries Real-world IoT implementations achieving results today*, SAS, 2016 https://www.sas.com/en_gb/insights/articles/big-data/3-internet-of-things-examples.html

[r] Larus, S. *5 Examples of How the Industrial Internet of Things is Changing Manufacturing*, Engineering.com, 2016 https://www.engineering.com/AdvancedManufacturing/ArticleID/13321/5-Examples-of-How-the-Industrial-Internet-of-Things-is-Changing-Manufacturing.aspx

[s] Roberts, F. *9 examples of manufacturers making IIoT work for them*, Internet of Business, 2016 https://internetofbusiness.com/9-examples-manufacturers-iiot/

[t] Shrouf, F., Ordieres, J., Miragliotta, G., *Smart factories in Industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm*, Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management, 2014

[u] R Woodhead, *4IR – The Next Industrial Revolution*, Digital Catapult / IoTUK, 2016

[v] Kosanke, K. *CIMOSA—overview and status*. Computers in industry **27**, 101-109, 1995

[w] Some examples are:
Siemens MindConnect https://siemens.mindsphere.io/
Dell's Edge Gateways http://www.dell.com/uk/business/p/edge-gateway
Beckhoff's TwinCAT solutions http://www.beckhoff.com/TwinCAT-Industrie40/

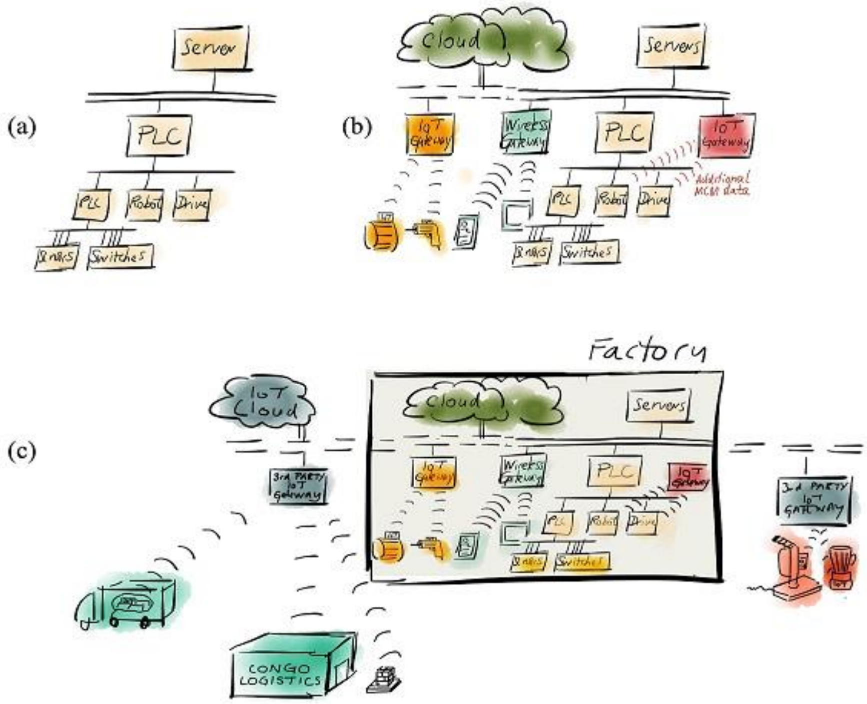


Figure 10: (Partial) Factory IT Architecture (a) Conventional (b) Extended to include local IoT (c) Further extension beyond the factory

3.4 Links to other Industrial paradigms

One of the challenges for both industrial users and academic developers in this area is the lack of distinction between numerous different paradigms. For comparability purposes we use the Wikipedia[x] definitions in all cases below)

Industry 4.0: Industry 4.0 is a name for the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of Things, cloud computing and cognitive computing. Industry 4.0 creates what has been called a "smart factory".

Digital Manufacturing: Digital Manufacturing is an integrated approach to manufacturing that is centred on a computer system.

Data Analytics / Big Data: Data analytics refers to qualitative and quantitative techniques and processes used to enhance productivity and business gain. Data is extracted and categorised to identify and analyse behavioural data and patterns, and techniques vary according to organisational requirements.

Cyber Physical Systems: A cyber-physical (also styled cyber physical) system (CPS) is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users.

Wireless Sensor Networks: Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organising the collected data at a central location.

The interaction between these definitions and the overlaps indicated diagrammatically in **Figure 11** highlight the challenge in defining a necessary programme of work in any one of these areas. With this in mind it might be convenient to restrict the

[x] https://en.wikipedia.org/

definition of IoT in an industrial context to being associated with:

(i) Edge: The development of sensing and actuation devices that attach to or represent properties of industrial equipment, products and materials

(ii) Gateway: connect (edge) devices such as sensors and actuators to local networks within the industrial organisation, and

(iii) Data Management Systems: the provision of (server or cloud based) systems required to manage and use the data associated with edge devices.

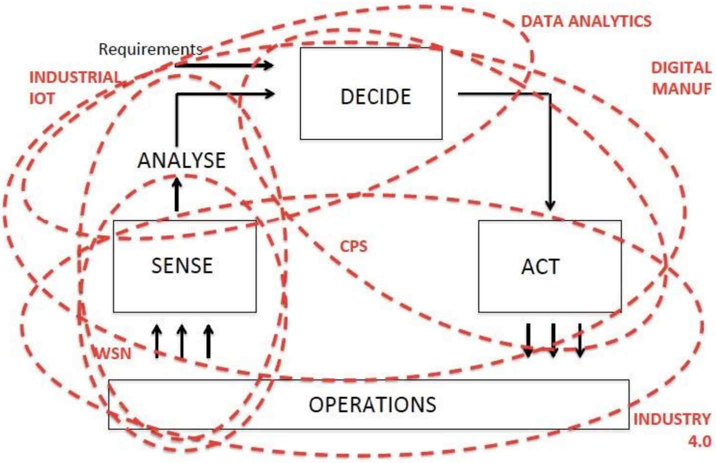


Figure 11: Digital Paradigms in Manufacturing

Such a restricted description would clearly provide a distinction from other digital paradigms such as data analytics and cyber physical systems – albeit providing data for the former and infrastructure for the latter. Its role in Digital Manufacturing and Industry 4.0 developments would be substantial but only part of what is required to address digital needs of the manufacturing industry.

3.5 Industrial IoT Research and Development

For reasons indicated earlier it is difficult to point to a set of activities in the UK directly targeting Industrial IoT developments. Indeed the major government report on IoT in 2014[y] didn't directly discuss industrial applications of IoT, a recent report by the Digital Catapult bundles IoT as part of the collection of paradigms identified in **Figure 11**, and the Innovate UK sponsored IoT Programme between 2013-16 focussed predominantly on city, business and domestic demonstrators and developments, although the HyperCat resource discovery standard[z] has some direct applicability to the industrial context. The EPSRC supported Petras: IoT Hub[aa] supports themes of general relevance to Industrial IoT (security, trust, privacy, economic value) and specifically has programmes of direct relevance such as *EVIoT* – Economic Value of IoT Data in Cyber-Physical Supply Chains and *IoT in Control* – Secure IoT Control Systems. Further IoT oriented research programmes are reported elsewhere[b]. Industrially, organisations such as Siemens, Rockwell, Microsoft, Dell and others are offering Industrial IoT systems and services. These generally refer to gateway devices that are compatible with the existing industrial IT backplane communications and provide mechanisms for shifting industrially generated data into cloud based data environments for analysis. The main application areas cited are those listed in Section 2.2 and monitoring, maintenance and asset management generally predominate.

The most well developed analysis of standards requirements for Industrial IoT stems from the Industrial Internet Consortium (IIC)[o] where a set of specifications in line with the common ISO Open Systems Interconnect standard[bb] are provided to handle the extension of Industrial Internet to integrate IoT developments.

It is expected that reporting of Industrial IoT applications and developments will accelerate significantly over the coming few years as the specific opportunities for Industrial IoT become clearer.

[y] A report by the UK Government Chief Scientific Adviser, *The Internet of Things: making the most of the Second Digital Revolution*, 2014 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

[z] PAS 212:2016, *Hypercat: Automatic resource discovery for the Internet of Things – Specification*, BSI Publications, 2016.

[aa] Petras: EPSRC Internet of Things Research Hub, https://www.petrashub.org/

[bb] ISO Open Systems Interconnect standard ISO/IEC, 7498-1:1994, http://standards.iso.org

3.6 Research Challenges in Industrial IoT

The areas for research discussed here are restricted to just those topics applying specifically to Industrial IoT. The reader is referred to other publications for the broader issues in IoT research,[b, x, z, cc] but we note that some issues, for example, IoT security, although generic are clearly relevant to Industrial applications for IoT. Figure 12 (taken from Miorandi, Sicari et al)[cc] identifies a broad taxonomy of general IoT research challenges which align roughly with the edge, gateway, server model used in this report.

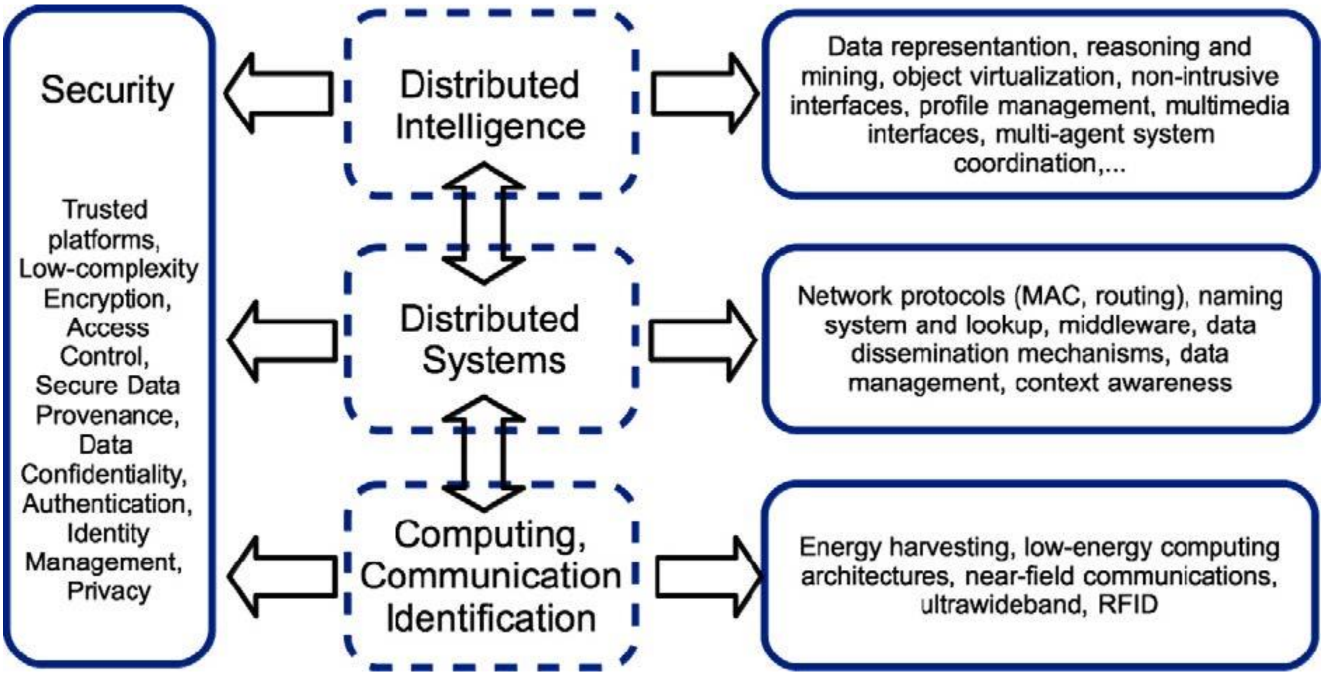

Security
Trusted platforms, Low-complexity Encryption, Access Control, Secure Data Provenance, Data Confidentiality, Authentication, Identity Management, Privacy
Distributed Intelligence
Distributed Systems
Computing, Communication Identification
Data representantion, reasoning and mining, object virtualization, non-intrusive interfaces, profile management, multimedia interfaces, multi-agent system coordination,...
Network protocols (MAC, routing), naming system and lookup, middleware, data dissemination mechanisms, data management, context awareness
Energy harvesting, low-energy computing architectures, near-field communications, ultrawideband, RFID

Figure 12: Taxonomy of research areas relevant to IoT

[cc] Miorandi, D., Sicari,S., De Pellegrini, F. and Chlamtac, I. *Internet of things: Vision, applications and research challenges*, Ad Hoc Networks, **10**, 1497-1516, 2012

We conclude with a set of potential research challenge areas specific to *industrial* IoT development.

- *Sensors and Actuators*[dd, ee]

Addressing issues of general relevance to all edge devices – e.g. energy consumption, latency, security, reliability –but viewing them through the lens of the industrial user. For example, eligibility, availability, timeliness of sensed data – especially that originating from outside the factory is critical if it is to be used within an automated industrial control environment or even if used as part of a maintenance regime.

- *Communications*[ff, gg]

The research community is awash with specific research relating to IoT communications issues such as latency, topology and safety. We would simply mention here that in addition to these issues is the need for guaranteeing real time availability of any IoT sensed.

- *Infrastructure*[bb]

Provision of an integrated and interoperable data management environment, allowing for data from multiple sources to be securely accessed and used by industrial operators, and managing the safety of any operation influenced by such IoT derived data is important. Conversely so too is allowing data gathered from industrial operators to be used by permitted 3rd party organisations. This latter issue is particularly important when the application of Industrial IoT to industrial products and services is being considered. The proliferation of different cloud-based data management environments[hh] is also setting new challenges relating to the interoperability and interfacing between different provider solutions.

- *Integration* [t, u]

Integration of evolving, new IoT developments need to be considered in conjunction with the existing industrial IT environments already operating. *Legacy management and migration pathways* for the secure introduction of additional IoT features needs to be established.

Further, understanding and exploiting the interface of IoT to the different digital manufacturing paradigms identified earlier (see **Figure 1**).

- *Standardisation* [e, z, bb. cc.]

The standardisation challenge is not so much in any one particular technical area but in (a) the development of a complete portfolio of standards (b) the industrial adoption of open standards to prevent proprietary approaches blocking development.

- *Economics* [ii, jj]

Of primary importance, is the need for an economic case that will clearly demonstrate benefits of introducing new IoT developments *over and above* those sensors and actuation offerings already available. Further, determining effective models for paying for the provision and access to sensed data. Further research is also required to support rather broad economic estimates that appear in the commercial domain.

Note that issues of *security, trust, privacy* and *safety* are mentioned under several of these categories and are tantamount to any successful deployments of Industrial IoT based systems.

[dd] Gubbia, J., Buyyab, R., Marusic, S., Palaniswami, M., *Internet of Things (IoT): A vision, architectural elements, and future directions*, Future Generation Computer Systems, **29**, September 2013

[ee] Flexeye, *Lord of the Things: Why Identity, Visibility and Intelligence are the Key to Unlocking the Value of IoT*, 2014 https://coe.flexeyetech.com/

[ff] Xu, L., He, W., and Li, S. (2014) Internet of Things in Industries: A Survey, IEEE Transactions. On *Industrial Informatics*, VOL. 10, NO. 4, November

[gg] IEEE Internet of Things Journal http://standards.ieee.org/innovate/iot/

[hh] For example, Siemens MindSphere *www.siemens.com/Mindsphere*,
Microsoft Azure https://azure.microsoft.com,
IBM Cloud https://www.ibm.com/cloud/internet-of-things

[ii] Ray, P.,P. *Creating Values out of Internet of Things: An Industrial Perspective*, Journal of Computer Networks and Communications, Article ID 1579460, 2016

[jj] McKinsey Global Institute, IoT: Mapping the Value Beyond the Hype. 2015

connected
everything.

industrial systems in the digital age

Connected Everything
Faculty of Engineering
University of Nottingham
University Park
Nottingham
NG7 7RD
UK.

www.connectedeverything.ac.uk