for a greener tomorrow

MITSUBISHI ELECTRIC
Changes for the Better

Industry 4.0 - The road to digitalisation in future manufacturing

Contents.

1.0: Executive summary

We are experiencing a fourth industrial revolution which is leading to the creation of what has been dubbed ‘Industry 4.0’ or I4.0.

The benefits which I4.0 can deliver for industry – and thus ultimately for consumers – include lower costs, faster production, better resource efficiency, higher quality control and greater product and component traceability.

The two key enabling technologies that will allow I4.0 to deliver these benefits are the Industrial Internet of Things (IIoT) and cyber-physical systems.

The IIoT enables multiple devices (as simple as a single sensor or as complex as a machine tool) to exchange data using Internet and Ethernet based technologies.

Cyber-physical systems are integrations of computation, networking and physical processes. In other words, the convergence of business systems with the physical plant control systems and machines. It is also about measuring actual performance against an “ideal model” or norm. with a range of new initiatives. Ensuring sufficient performance is also a key requirement which early adopters of I4.0 need to consider.

I4.0 and its supporting technologies are not without challenges, however. Issues such as the need for better security and permitting systems from multiple vendors to work together are being tackled

Manufacturers need to consider the current levels of manufacturing plant automation and network architecture that exists within the plant today. Adopting the principles of I4.0 and smart manufacturing requires high levels of automation and network infrastructure so the road to digitalisation can require high levels of investment.

Governments and industry around the world have recognised the potential of I4.0 (also known by a variety of other names worldwide) to change the competitive landscape. New organisations have been set up to direct and support development of I4.0 and substantial private and public sector investment is being made.

This white paper sets out to explain the background, consider the challenges and offer solutions to the adoption of I4.0 related technologies and solutions.

2.0: Industry 4.0 (I4.0) and the industrial Internet of Things (IIoT)

The first industrial revolution, which began in the UK in the 18th century, was characterised by the widespread adoption of steam power and the mechanisation of production.

There was a second industrial revolution in the early 20th century when 'mass production' became dominant, pioneered by US automotive manufacturers such as Henry Ford. A 'third industrial revolution' began later in the 20th century when programmable electronic systems and computer technologies helped to further automate production lines.

Now we are experiencing the fourth industrial revolution. It is based on hugely increased sharing of data across multiple systems and between participants in the manufacturing process – and the benefits that arise from this.

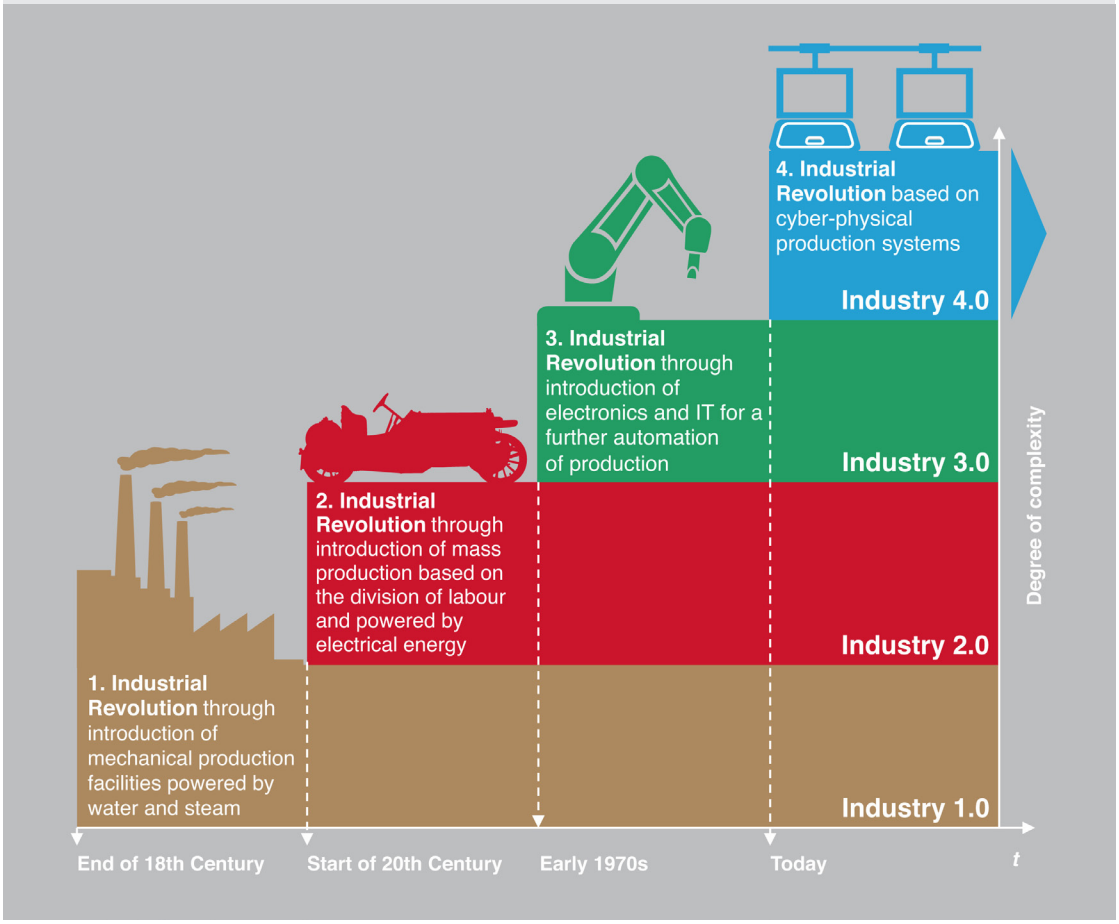
2.1: The basis of I4.0

I4.0 brings together two linked and rapidly advancing technologies – cyber-physical systems (see Section 2.6) and the IIoT, the Industrial Internet of Things (see section 2.4). It is based on a number of overlapping principles:

- Interoperability: Allowing machines, devices, sensors, organisations and people to connect and communicate with each other via the common standards and protocols of the IIoT.
- Information: Using an information system based on a 'virtual model' of the physical world working in real time with a wide range of data – including data from sensors which may be part of cyber-physical systems.
- Integration: Assisting decision-making by aggregating data from multiple sources and presenting it in a comprehensible format for management decision-making.
- Automation: Further extending the automation of 'Industry 3.0' by reducing the need for humans to undertake tasks which are unpleasant, repetitive or potentially risky.
- Autonomy: Removing humans from decision-making and manufacturing processes by making use of the ability of cyber-physical systems to make decisions on their own in response to things happening in the 'real world' manufacturing environment.

Key features of I4.0 include:

- ‘Vertical’ networking of production systems, logistics, procurement and other industrial and business processes – extending, perhaps, into marketing and after-sales support.
- ‘Horizontal’ networking of systems, linking multiple participants in the production process (both individuals and organisations) including designers, manufacturers, suppliers, warehousing, logistics, customers – and ultimately, perhaps, consumers.
- Integrated engineering in which all the horizontally linked participants in the production process share common data, facilitating development of new designs, production systems and business models.
- Acceleration of new technology adoption throughout the design, production and supply process.



I4.0 brings together cyber-physical systems and the Industrial Internet of Things.

2.2: The rise of I4.0

I4.0 is being driven by market forces including the needs to cut manufacturing costs, increase efficiency, make better use of resources, improve flexibility and reduce 'time to market'.

Particularly in 'developed' countries where labour costs can be high, I4.0 can maintain or improve manufacturing competitiveness by increasing automation and therefore productivity, while also helping to maintain or increase quality.

I4.0 also permits manufacturers to respond to the increasing consumer demand for personalisation – so-called 'mass customisation'.

In a factory producing motor vehicles, for example, it is now rare to see two identical models follow one another down the production line. Each is built to an individual specification to match the requirements of a specific customer. Variations can range from quite major changes (such as a different engine size) to relatively minor modifications such as a different interior trim.

The same requirement for mass customisation is now being met in a variety of sectors from toys to medical devices such as spectacles where each lens must be adapted to an individual's prescription. You can even order customised breakfast cereals with the precise ingredients just how you like them!

In I4.0 these variations can be accommodated without a significant change in manufacturing cost compared with producing batches of identical models.

2.3: The role of Data Communication

I4.0 requires the sharing of huge amounts of data at high speed between many participants in the manufacturing process – be those individual machines, people or organisations.

The predominant technology for data communication within I4.0 is Ethernet.

Ethernet was developed as a system for connecting a number of computers and other devices, such as printers, to form an office network with protocols which control the passing of information between them.

One of Ethernet's key original features was that it enabled all the devices on the network to communicate with every other device over a single cable. The network could be expanded to accommodate new devices without requiring any modification to those devices already connected.

Originally developed in 1973, Ethernet has now become an international standard for commercial networks – including, importantly, the internet – and is increasingly used in industrial networks which (for example) connect all the machine tools on a factory floor.

Industrial control networks originated in the 1980s when what became known as ‘fieldbuses’ began to appear. These were based on serial communications technology and were designed to replace complex and costly control systems which required individual sensors, actuators, controllers and machines to be separately wired together to create a bespoke network. In essence, a fieldbus allowed all these devices to pass data over a common set of wiring or ‘bus’, significantly reducing the amount of cabling, simplifying maintenance and reducing cost. A fieldbus also made future changes far easier, significantly increasing flexibility.

Many different fieldbuses appeared and they remain at the heart of industrial networking. The International Electrotechnical Commission (IEC) sets standards for these protocols and many other aspects of industrial networking[1].

All the leading fieldbuses and the industrial network systems which have developed from them, are now ‘open’ systems – ie, all the underlying technology is available for anyone to use. The companies which originally developed these systems have handed control of the technology to external bodies which now manage and maintain it.

This move to open systems has been driven by user demands and by economic and commercial realities.

Users want open systems to ensure they are not ‘locked in’ to a single supplier with all the business risks that this would entail.

The companies that originally developed the systems see benefits in providing open access to their technology because it enables a wide range of vendors to develop equipment using these standards. This makes the standards more attractive to end-users because of the wider choice of software and hardware – which is developed and marketed without cost to the original developer of the standard. Equally of course, each sale of an industrial network built on one of these standards often involves the purchase of substantial amounts of equipment from the originator.

These same commercial and technical pressures have led all the fieldbus systems to move to adoption of Ethernet as a common physical layer. However, there are significant differences between ‘industrial’ and ‘commercial’ Ethernet systems.

One key difference is the physical ruggedness required of industrial systems which may be subject to temperature extremes, vibration, physical contamination and electronic ‘noise’ from their environment which are not found in the offices and homes for which Ethernet was developed.

Another key difference is the need for ‘determinism’ in industrial systems – the ability to ensure events occur exactly as planned, even at very high speed. This is explored further in Section 2.5.

Despite this, Ethernet has evolved to embrace these challenges and has become the ‘de facto’ standard for data communication within I4.0, facilitating data exchange between ‘industrial’ and ‘commercial’ systems – and opening the possibility of future communication directly with consumers.

2.4: The Industrial Internet of Things (IIoT)

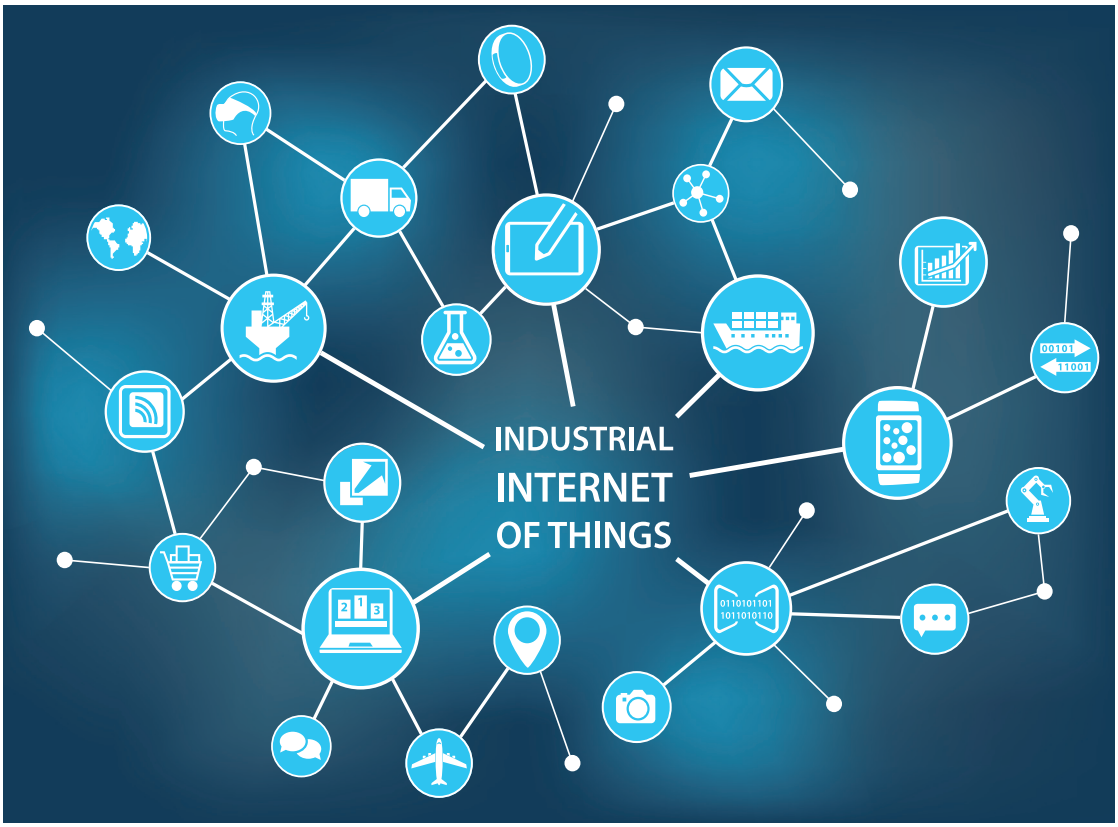
A key enabling technology for I4.0 is 'the Industrial Internet of Things' (IIoT).

Until recently the internet was chiefly concerned only with connecting computers and associated devices, such as printers, allowing them to view and share electronic versions of documents or other digital data, such as audio and video files. Ethernet technologies enabled many of these connections.

As the widespread adoption of these technologies has caused their cost to fall, the same technology has been incorporated into a wide variety of devices that are not traditional computers. Hence mobile phones, heating thermostats, cars and even light bulbs are now able to communicate with other similarly equipped devices using internet technologies. This is the basis for what has become known as 'the Internet of Things' (IoT).

This trend is expected to continue and we will therefore see an ever broader variety of devices, systems and machines communicating in this way.

That philosophy of inter-connectedness also runs through the manufacturing version of the Internet of Things – the Industrial Internet of Things (IIoT) which brings together a number of broad trends such as machine learning, 'big data' and machine-to-machine communication.



The Industrial Internet of Things (IIoT) will make machines smarter.

The underlying idea is to make the machines which power our economy 'smarter' by gathering and analysing data and then making appropriate responses, often in real-time. It is this need for real time performance that distinguishes the IIoT from the IoT in the same way that commercial Ethernet is usually not suitable for an industrial environment.

Thus a pump in a sewage station connected to the IIoT might signal for a service call when it detects a bearing starting to run hot, preventing a subsequent failure of the bearing and allowing shut-down and servicing to be scheduled when least disruptive. It is an IIoT application analogous to the probably most-quoted example of the commercial IoT, the refrigerator which notifies its owner when more fresh milk needs to be purchased.

Equally. just as the next development of the IoT might permit the fridge actually to place an order for milk with the supermarket, with no human intervention, the next development of the IIoT may allow the sewage pump station to call a service robot.

A recent report from consultancy Accenture[1] includes a prediction that the value created by the IIoT could be as high as US$15 trillion of global GDP by 2030.

2.5: Determinism

For many IoT consumer applications, speed and real-time communication are useful but not critical. If your refrigerator does not immediately detect a shortage of fresh milk and submit an order to the supermarket within a few milliseconds there will be little problem caused by the delay.

In an industrial system, however, the timing of data transmission can be critical. For example, a warning from a machine tool that it has for some reason failed fully to offload the component it has just manufactured must reach the robot seeking to load the next component before it makes the attempt.

High speed packaging machines that are filling, for example, jars or bottles with food products in seconds (or fractions of seconds) actually need millisecond level precision in the timing of signals that control the process of placing, filling, removing and sealing the containers. Missed connections and millisecond delays in communication between robotic systems can cause products and perhaps production machines to become unsynchronised, often leading to damaged products or even damaged machines.

Even more catastrophic consequences might flow from, for example, the failure of a system to respond immediately to a warning of over-pressure in a boiler.

Industrial systems therefore need true 'determinism' – the ability to guarantee an event will occur precisely when expected. It is essential to ensure that events happen exactly when they are supposed to happen and that there is no scope for variability or 'jitter'.

That is not always the case with ‘commercial’ Ethernet which uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD) to control the flow of information on the network.

Every device on a commercial Ethernet network has equal access and can try to place data onto the network without any consideration of what another device is doing. If two devices try to add data to the network at the same moment, one must back off and wait before trying again. It is this inherent variability which prevents determinism.

Hence although the CSMA/CD protocol avoids data loss it means that Ethernet is normally ‘non deterministic’ – there is no control over the timing of data transmission.

Several recently introduced protocols have brought the necessary level of determinism to industrial Ethernet applications. However, as greater levels of connectivity and new industrial process automation methods are developed to fulfil the potential of I4.0 and the IIoT, bandwidth issues will become the key focus, as determinism is now a given.

The Institute of Electrical and Electronics Engineers (IEEE) has set up a Time Sensitive Networking (TSN) task group[2] to create an industry standard on this issue.

Industrial systems need true determinism.

2.6: Cyber-physical systems

The second key component of I4.0 alongside the IIoT is the development of cyber-physical systems. These bring together mechanical and software based analytical elements to create what was formerly called a ‘mechatronic’ system.

However, cyber-physical systems go way beyond the coming together of mechanical and control system components as previously defined as a mechatronic system.

Cyber-physical systems are constantly comparing the actual performance of the machine or process with the required ideal performance or norm. The difference between the measured performance and this reference model is detected automatically by the system. This can lead to several outcomes but it can be summarised as anomalies that can be automatically corrected by the control system itself, in other words the system thinks for itself and corrects the problem, or it highlights deficiencies in the process which may lead, following analysis over time to changes in the operation methodology.

It is the convergence of the enterprise level of the business to the manufacturing plant in this way that separates the cyber-physical system from we have understood in the past.

Thus the sewage pump station mentioned above in Section 2.4 is part of a cyber-physical system. It has mechanical elements such as a sensor which detects the bearing vibration. This vibration is then analysed by an analytical software based system which decides if the vibration is heading out of specified limits. It then uses IIoT-based principles to warn maintenance staff that maintenance should be completed soon. This example relates to predictive maintenance rather than production throughput but still illustrates the classic cyber-physical model.

2.7: New computing models

'Cloud computing' – using a network of remote servers hosted on the internet to store, manage and process data, rather than using a local server or a personal computer – has become familiar in office and commercial systems. It will play a significant role in I4.0 for all the same reasons that it is becoming common in other applications:

- Reduced cost (servers can be shared across multiple applications).
- Scalability (applications can use as much or as little computing power as they need at any instant).
- Reliability (new servers can be switched in seamlessly in the event of a hardware failure).
- Ease of data backup.
- The ability to easily upgrade to the latest hardware and software.

Another computing technology which is frequently associated with I4.0 is 'edge computing' and the related 'fog' and 'dew' computing.

In line with the underlying philosophies of I4.0 (see Section 2.1) edge computing moves applications, data and computing operations away from centralised points or 'the cloud' and puts them as close as possible to the systems being controlled. This relocation of computing power can be both conceptual in the way systems are designed and also physical in terms of the real-world location of devices.

This significantly decreases the volume of data that must be moved and the distance that it must travel, thus reducing transmission costs and 'latency' and improving determinism.

2.8: Standards

To make I4.0 and the IIoT function, software and hardware from multiple vendors must be able to exchange data in a way which can be 'understood' by all parts of the system.

Part of the solution is common use of Ethernet (see Section 2.3). However, currently Ethernet primarily addresses the 'physical layer' – the actual cables (or wireless connections) and associated standards that allow traffic to flow on the network. A complementary technology that governs how devices and systems communicate with each other over the network at a high level is required. This is OPC – which originally stood for OLE (Microsoft's Object Linking & Embedding) for Process Control.

The OPC Unified Architecture (UA), released in 2006, is an interoperability standard for the secure and reliable exchange of data in industrial automation. It is platform independent and ensures the seamless flow of information among devices from multiple vendors.

The OPC Foundation is responsible for the development and maintenance of this standard which is a series of specifications developed by industry vendors, end-users and software developers. These specifications define the interface between clients and servers, as well as between different servers, including access to real-time data, monitoring of alarms and events, access to historical data and other applications.

It may be that the future of industrial networks will be based on a combination of TSN (see Section 2.5) and OPC UA in which TSN defines the physical layer of networks and OPC UA defines the software.

Further development of international standards is expected as an outcome of the meeting held in March 2016 which brought together representatives of Germany's Platform Industrie 4.0 and the Industrial Internet Consortium. The two organisations aim to align their two 'architectures' – the Reference Architecture Model for Industrie 4.0 (RAMI4.0) and the Industrial Internet Reference Architecture (IIRA) – to ensure future interoperability[3].

3.0: Opportunities and challenges with I4.0

I4.0 offers tremendous opportunities to manufacturing industry including lower costs, faster production, better resource efficiency, higher quality control and greater product and component traceability – but I4.0 also poses challenges.

3.1: The challenges of I4.0

The challenges of I4.0 for manufacturing industry include investment, skills, technology and security.

Manufacturing plant is often a long-term investment. Production facilities are not easily or cheaply replaced and manufacturers seek to keep factories and machines operating for as long as economically and technically possible to maximise return on investment – typically 20 years in some cases.

Building I4.0 into a new plant adds proportionally little to costs and can show a swift return on the investment. Adding I4.0 capabilities to an existing production facility could be a large investment which needs careful analysis to determine whether it will give a worthwhile pay-back over the remaining operational life of the plant.

The challenges of adding I4.0 to an existing plant should not be underestimated.

Much will depend on the level of automation and network infrastructure that already exists.

I4.0 and smart manufacturing depends entirely on the data exchange between the plant and the business level systems for production analysis and preventative maintenance and the like.

Many manufacturing plants have been around for many years and in the past did not focus too much on the requirements of automation and data gathering.

What is encouraging however is that the technology to deliver against the requirements of I4.0 exist today and with planning and a structured approach, can be applied to any manufacturing plant (see Section 6.0).

Introducing I4.0 into either new or existing plant may require new skills from the workforce that merge current manufacturing and IT specialisms.

Increasing levels of automation and autonomous decision-making that are at the heart of I4.0 will reduce the need for some existing production skills. However, specifying, installing and maintaining the I4.0 hardware and software will require a different skill-set with a much higher requirement for IT expertise. Manufacturers may need to recruit and/or train appropriate personnel and/or find suitable outsourced suppliers.

With both investment and training, manufacturers must look to the future and predict what new technologies may come to market in the years ahead and how these can be integrated into I4.0 systems being installed today. The ‘open source’ nature of much of the current technology (see Section 2.8) means users need not be as concerned as in the past about commitment to a particular

vendor but there is still merit in developing long-term relationships with suppliers of critical systems.

Security is a major concern for development of I4.0. The 'inter connectivity' envisaged by I4.0 and the IIoT opens companies to new possibilities of malicious internet-based attack. Ironically, the adoption of common standards such as Ethernet which are essential for the success of I4.0 and the IIoT also create security vulnerabilities – hackers as well as vendors and users can easily transfer their skills from one system to another.

Industrial networks have been compromised by the sort of threats that have seen high-profile breaches of commercial systems – threats such as unauthorised access and operation. These can come either from within an organisation or from an external source and can be either malicious or accidental.

The problems of hacking from within a company are as much a personnel security issue as a general network security issue. Security considerations need to consider both deliberate acts of sabotage and the possibility of personnel making a mistake.

One benefit of I4.0 that is already being exploited is the ability to monitor and control production plants and other equipment from a remote location. However, current monitoring processes typically use standard web browsers, which open the system up to the possibility of abuse of the network by third parties.

The risks of poor network security extend beyond purely economic ones. Hackers taking control of the management systems for industrial plants could cause significant damage while themselves being safely located on the far side of the world.

A recent report from the UK's Institution of Mechanical Engineers noted that manufacturers of industrial control systems have not traditionally focused on security because these systems were typically 'stand-alone' and not accessible via the internet. The report noted also that these systems usually have a long lifetime, often exceeding the vendor's support periods for the platforms they are built on. There is a risk of unsupported systems not being updated to address evolving security vulnerabilities[4].

The industry is, however, responding to these threats. The IoT Security Foundation (IoTSF) has been established to develop a collaborative and international approach to security[5].

Meanwhile, a number of technology firms have recently joined forces to develop a management protocol for IoT devices that could pave the way to an open, interoperable standard to address security and privacy risks. The Open Trust Protocol (OTrP) combines secure architecture with trusted code management, using technologies proven in sectors such as banking and in mass-market devices such as smartphones and tablets[6]. It is likely that many of these initiatives will be transferred to the industrial sector and the IIoT.

As an example, the German Federal Office for Information Security (BSI) – the nation's cyber security authority – recently tested OPC UA (see Section 2.8) and found the security to be good[7].

4.0: The current and future state of I4.0

Governments and industries across the world have recognised the potential of I4.0 to transform economies. New organisations and initiatives, often bringing together both the public and private sectors, are being established worldwide to reap the benefits of I4.0.

4.1: Current level of adoption

China

In 2015 the Chinese government launched its 'Made in China 2025' initiative[8]. Premier Li Keqiang said: "We will implement the 'Made in China 2025' strategy, seek innovation-driven development, apply smart technologies, strengthen foundations, pursue green development and redouble our efforts to upgrade China from a manufacturer of quantity to one of quality."

A total of 15 innovation centres will be established by 2020 (and 40 by 2025) focusing on digital manufacturing as well as broader IT, new materials and biotechnology. All will be supported with government funding.

The plan says that China will aim for a big leap in innovation as well as manufacturing efficiency. It aims to compete with developed manufacturing powers by 2035 and lead the world's manufacturing by the 100th birthday of the 'New China' in 2049.

Germany

The concept of I4.0 was first announced at the Hannover Fair in 2011 and received the personal backing of Chancellor Angela Merkel[9].

The country now has a number of programmes bringing industry and government together to advance the concept.

Government-funded 'centres of competence' were established from 2015 across the country to lead development of I4.0.

Development of I4.0 is now led by Platform Industrie 4.0 which aims[10] to "continue the German government's high-tech strategy and to support its implementation in Germany, thus maintaining the country's position as a leading production location."

Platform Industrie 4.0 is managed by VDMA (Verband Deutscher Maschinen- und Anlagenbau), the mechanical engineering industry association which represents over 3,100 mostly medium-sized companies in the capital goods industry, with support from Bitkom, Germany's digital industry association and ZVEI, the electrical industry association which has a large number of members involved in industrial automation.

India

A report[11] prepared for the Confederation of Indian Industry suggests that the country's manufacturing sector is generally ill-prepared to embrace I4.0.

However, the Indian government's 'Make in India' initiative[12] has laid out new policy initiatives to expand the economy's manufacturing capabilities. The initiative includes creating a conducive environment for technological evolution.

Japan

Research[13] suggests that Japanese firms lag behind their European and American competitors in embracing I4.0.

However, a consortium of about 30 Japanese companies including Mitsubishi Electric, Fujitsu, Nissan Motor and Panasonic have launched a new forum[14] – the Industrial Value Chain Initiative – to create standards for technology to connect factories and efforts to internationalise Japanese industrial standards and to standardise security technology.

The Japanese government, several industry associations and leading companies have launched the Robot Revolution Initiative (RRI)[15]. Its definition of 'robot' extends beyond popular use of the term to include advanced manufacturing technologies.

Korea

In Korea the government's Innovation in Manufacturing 3.0 programme[16] includes an investment of US$172 million annually with a target to build 1,500 smart factories by 2020. The programme is focused on support for small and medium enterprises (SMEs) with a view to disseminating smart factory technologies among these companies.

Taiwan

The Taiwan Electronic Equipment Industry Association (TEEIA) has formed an I4.0 group[17] that will be geared toward fostering development of smart factory and production processes in Taiwan in order to help local manufacturers stay competitive in the world market.

The Taiwanese government's Industrial Development Bureau (IDB) under the Ministry of Economic Affairs has established ties with leading German companies[18] with the aim of establishing Productivity 4.0 alliances in Taiwan.

United Kingdom

A recent survey[19] undertaken by consultancy BDO and the Institution of Mechanical Engineers found that only eight per cent of a sample of engineers in management or director level posts in UK industry had a 'good understanding' of I4.0 and 56 per cent had 'little or no understanding'. Only 20 per cent of responding companies had some form of I4.0 strategy in place.

The UK government has established 'high value manufacturing catapult centres' across the UK and these centres have taken on a role as thought leaders and proponents of I4.0.

The government has already announced plans to establish an Institute for Coding which will help to support digital skills.

United States

I4.0 is promoted in the USA through the Advanced Manufacturing Partnership (AMP), which was launched by President Obama in 2011, and the Industrial Internet Consortium (IIC).

The IIC has more than 150 members, including many Asian and European companies. It aims to "coordinate and establish the priorities and enabling technologies of the Industrial Internet in order to accelerate market adoption and drive down the barriers to entry". Its work is directed by 19 working groups and teams, broken into seven broad areas which include topics such as legal and marketing as well as technology and security[20].

The Smart Manufacturing Leadership Coalition (SMLC)[21] aims to "build the nation's first Open Smart Manufacturing Platform for collaborative industrial-networked information applications through at-scale demonstrations."

The SMLC's Open Smart Manufacturing Platform and Marketplace gives manufacturing companies access to modelling and analytical technologies.

Switzerland

A report from consultancy Deloitte[22] says that the transformation to I4.0 in Switzerland is "making partial progress".

A survey of the country's manufacturing business which the firm undertook in 2015 found, for example, that the majority of companies were already feeling the impact of I4.0 and that 32 per cent said their IT infrastructure was ready to support a move to I4.0.

4.2: The future for I4.0

Predicting the future is always difficult, particularly in technology markets where a single new development can disrupt whole industries. However it is possible to confidently predict something of the future for I4.0 and the IIoT from current emerging trends.

- The IIoT will grow swiftly (as will the more general Internet of Things in consumer markets) with more and more devices being connected.
- There will be a massive growth in data, not just because of the growth in the number of connected devices but because of the increasing amount of data that the devices individually will generate.
- There will be a consequent growing demand for bandwidth on and between industrial networks. Again, one can look at consumer markets for parallels. As devices capable of handling more data become available, so applications that will use that capability are developed. Streaming video (YouTube, Netflix and others) to mobile phones now requires both the devices and the connecting networks to have huge bandwidth that was not required only a very few years ago. In the business-to-business market we have seen, for example, aero-engine makers such as Rolls-Royce set up systems to capture data in real time from engines flying around the world and analyse it for clues to future maintenance needs.
- Security will become increasingly important as the ability to create havoc – either deliberately or accidentally – via the IIoT increases.
- International standards to ensure interoperability will become increasingly important, driven by market demands from equipment vendors and end users. Standards will converge around developments of Ethernet for the industrial environment.

Existing industrial control networks (based usually on the current standard bandwidth of 100 Mb) are unlikely to be able to handle the amount of data generated in the near future. The obvious solution is a step change in the bandwidth available on the network to gigabit speeds, supplied for example, by network technologies such as CC LINK IE offered by the CLPA (CC LINK Partners Association)[23].

5.0: I4.0 network requirements and solutions

The requirements for performance in industrial networks are far higher than in commercial networks (see Section 2.3). However, the Ethernet technology developed for commercial systems is now the basis for established standards in industrial systems (see Section 2.8) due to the on-going evolution of the technology.

5.1: The future Ethernet requirement

It is clear that future industrial control networks which will be central to I4.0 will be based on Ethernet. It is an international standard that will ensure interoperability of industrial and commercial networks and make possible the Industrial Internet of Things.

What, though, should be the characteristics of a future 'industrial Ethernet' for I4.0 and the IIoT? It must be:

- Physically robust enough for the production environment.
- Deterministic (see Section 2.5).
- Capable of delivering the bandwidth necessary not just for current levels of data transmission but for the increasing levels that I4.0 and the IIoT will require in future. This will include both synchronous and asynchronous data. Synchronous (or 'cyclic') data is the 'routine' control data on the network which will grow with the increasing number of devices and the increasing amount of data each will generate. Aysnchronous (or 'transient') data arises from things such as alarm conditions which generate short-term peaks of data. High bandwidth is needed to be able to deal with both simultaneously without losing data.
- Open standards-based to ensure easy interoperability in a multi-vendor environment.
- Secure against malicious attack.
- Fault tolerant.
- 'Backwards compatible' with earlier technologies – in particular, with fieldbus systems.

5.2: Choosing the right network

Despite the convergence of standards which are increasing the interoperability of networks and hardware from multiple vendors, developing hardware to operate on all available industrial network standards is still impractical for producers of industrial products. They typically focus on a small group of standards and technologies that will provide the most commercial success based on market demand.

End-users – companies which run factories and process plants – often choose just one standard. Certainly, in any single plant, it makes technical and economic sense to have a single standard as far as possible. There are also strong arguments (such as transferability of skills, personnel and spare parts) for companies operating multiple plants to use the same industrial control network on all their sites.

How then should equipment vendors and end-users choose between the systems on offer?

The choice comes down to two factors – the technology and the commercial benefits.

6.0: The road to digitalisation

As already discussed in Section 3.1, building a new plant and adopting the principles of I4.0 and smart manufacturing is achievable using the technologies available to us today. However, embarking on a project to bring an existing manufacturing plant to “smart factory” status is an altogether different prospect.

There are many challenges to overcome to achieve this but with the correct planning and structured approach it is possible to convert an aging plant into a smarter factory.

6.1: Understand the current situation

It is vital to understand the current situation with the plant.

All plants will be different and some will already have a good deal of automation and network architecture present. Many however will not and this section will deal with the latter.

Start with a survey of the plant assets and network infrastructure, if one exists.

Unless a site wide specification exists, it is likely that machines and other plant assets will be controlled by different vendor’s automation solutions.

A common network strategy may exist but it is unlikely that this is comprehensive enough for an I4.0 strategy.

Once this picture of the current situation has been obtained a strategic plan can be developed

6.2: Strategic Planning

It is extremely important to understand what the manufacturer is trying to achieve and also where are the “pinch points” for them

Sometimes the areas giving the most concern are not related directly to automation but may be operational issues in the manufacturing process.

To bring a mature manufacturing plant to a smart factory is likely to require significant investment and it is important to understand that this process may take a long time to realise.

It is therefore important to develop a strategic plan which allows the project to be completed in stages whilst maintaining a “big picture” view of the end goal.

It is also important to focus on some quick wins.

If the plant is currently achieving its production targets then there may be a view of “why do we need to be smart?”

If there is a clear understanding of the pinch points then it should be possible to focus on something that will give a quick return on a limited investment, this will go a long way to convince the people holding the budgets that moving towards smart manufacturing is the right thing to do.

Much of what is needed is data capture and a basic network infrastructure is mandatory but conceiving a flexible network architecture should allow areas of the plant to be tackled one at a time.

Overlaying a data gathering system on top of the plant automation layer can be done relatively unobtrusively. This largely depends of course on whether the required data is already being collected at the asset but in any case this requirement is often over and above the asset control program.

The I4.0 concept and the smart factory is about convergence of the enterprise level of the business and the manufacturing plant and tying in the business eco systems in a “smart” way.

However, in order to achieve that the fundamental requirement is to fully understand what is happening at the production plant.

A good maxim to adopt is “first visualise the plant then worry about the cloud.”

Implementing the correct automation and network architecture allows this to happen and enables the possibility of cyber-physical systems further down the line.

With a structured approach and clear goals it should be possible to implement this strategy over time with a phased approach, allowing budgets to be raised for each phase.

What must however be communicated very clearly is the end goal and the business benefits to the manufacturing plant.

7.0: Conclusions

Technology exists today that can make I4.0 a current reality. The speed and scale of future technology development ensures that I4.0 will become a common feature of manufacturing industry within a few years.

The benefits of adopting an I4.0 strategy to deliver smart manufacturing is clear; increased efficiency, increased productivity, increased flexibility, reduced downtime, reduced time to market, greater competitiveness and increased profitability.

The road to digitalisation to achieve these goals may be challenging but by approaching the task in a structured manner and ensuring that return on investment can be seen for each phase of the project, delivering smart manufacturing is very possible to achieve today and with further technological advances guaranteed, what will be possible will clearly change the way we operate in the future.

Just as ten years ago the thought of watching TV over the internet seemed unbelievable, manufacturing will also come to depend on services that have not yet even been thought of.

The next ten years will be extremely interesting and it is an exciting time to be involved in technology and manufacturing.

8.0: References

1. https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf
2. http://www.ieee802.org/1/pages/tsn.html
3. http://www.plattform-i40.de/I40/Redaktion/EN/PressReleases/2016/2016-03-02-kooperation-iic.html
4. http://www.imeche.org/docs/default-source/1-oscar/reports-policy-statements-and-documents/bdo-industry-4-0-report
5. https://iotsecurityfoundation.org/
6. http://rethink-iot.com/2016/07/21/open-trust-protocol-aims-iot-security-consolidation/
7. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2016/Sicherheitsanalyse_OPC_UA_26042016.html
8. http://www.scmp.com/tech/innovation/article/1818381/made-china-2025-how-beijing-revamping-its-manufacturing-sector
9. http://www.euractiv.com/section/digital/news/merkel-calls-for-industry-4-0-at-german-it-summit/
10. http://industrie40.vdma.org/en/article/-/articleview/4262621
11. https://www.mycii.in/KmResourceApplication/42511.CIIRolandBergerIndustry40.pdf
12. http://ww2.frost.com/news/press-releases/industry-40-make-india-frost-sullivan-sps-automation-india-2015-gandhi-nagar/
13. http://www.japantimes.co.jp/news/2016/04/29/business/examining-industry-4-0-opportunities/#.V6B8FZRTGUn
14. http://asia.nikkei.com/Business/Trends/Japan-launches-forum-to-counter-German-initiative
15. https://www.jmfrri.gr.jp/english/outline/establishment.html
16. http://www.businesskorea.co.kr/english/news/ict/13092-interview-secretary-lee-gyu-bong-uniqueness-korea%E2%80%99s-industry-40
17. http://www.svmi.com/taiwan-pushing-industry-4-0-developments-geared-toward-smart-production/
18. http://www.moea.gov.tw/Mns/english/news/News.aspx?kind=6&menu_id=176&news_id=54376
19. http://www.imeche.org/docs/default-source/1-oscar/reports-policy-statements-and-documents/bdo-industry-4-0-report
20. http://www.iiconsortium.org/index.htm
21. https://smartmanufacturingcoalition.org/about
22. http://www2.deloitte.com/content/dam/Deloitte/ch/Documents/manufacturing/ch-en-manufacturing-industry-4-0-24102014.pdf
23. https://eu.cc-link.org/en/

for a greener tomorrow

MITSUBISHI ELECTRIC
Changes for the Better

Hatfield Headquarters Contact: Mitsubishi Electric Europe B.V., Automation Systems Divisions, Travellers Lane, Hatfield, Hertfordshire AL10 8XB
Tel: +44 (0) 1707 288769 Fax: +44 (0) 1707 278695 / Web: gb3a.mitsubishielectric.com / Email: automation@meuk.mee.com