Going Fourth

Data, Industry 4.0 and the
Future of Manufacturing

IM irwinmitchell

Get Yourself Connected

If you can measure and understand it, you can use it to improve. This is the business case for digitalisation, a trend enveloping us all.

Get Yourself Connected

Until fairly recently the concept of a fully 'lights-out' smart factory was confined to a handful of high-tech companies and a few YouTube videos showing automated vehicles in modern factories sparsely populated by humans. This concept has now moved into reality.

By 2025, one report says there'll be 26 billion connected devices on the planet, or more than three devices on average for every single person.

In January 2019, the World Economic Forum published its 'Beacons of Technology' report, covering exemplar modern digital factories – real-life practitioners of Industry 4.0 manufacturing. The list includes BMW, Bosch, Danfoss, Fast Radius, Foxconn, Haier, Johnson & Johnson, Sandvik Coromant, and more, and spans locations worldwide.

While none of these 'lighthouse' factories are located in the UK – and with only one, DePuy, in Ireland – we're now seeing the rise of connected factories here. Mettis Aerospace, a mid-sized supplier to the aerospace sector, is building a digital factory using Wi-Fi 6. Grainger & Worrall, a £50 million castings business for the motorsport industry, is working with Warwick Manufacturing Group on a new fully-connected factory. Many more are linking what they do on the shop floor to the whole business wirelessly and instantly.

This ultra-connectivity is producing more and more data – petabytes of it. Domo, a US company that connects business processes to smartphones, estimates that 2.5 quintillion bytes of data is being produced every day. As the number of devices connected to the Internet of Things (IoT) rises, so will the amount of data. By 2025, one report says there'll be 26 billion connected devices on the planet, or more than three devices on average for every single person. Other estimates are even higher.

Machines in factories and farms – machine tools, presses, laser jet cutters, 3D printers, robots, material conveyors, agricultural machinery and condition sensors – are being connected, and sharing their data with an enterprise system or systems. Software is being developed to interpret and value this data – companies have never had so much accurate information about their operations as they do today.

But with volume comes risk. There are greater opportunities for cyber criminals to compromise data and plant malicious code. The risk of valuable data leaking or being lost is also rising in proportion to the volume.

In this report, we address the Fourth Industrial Revolution (4IR) from the perspective of data. We comment on what industrial data is, how to value it, international standards, cyber security practices, and aspects of the law relevant to data ownership and transmission. We also present several case studies from organisations with expertise in digital factories, data management and cyber security.

We hope you find the report useful. Please get in touch if you'd like to find out more.

Melanie Bancroft
Business Development Manager
melanie.bancroft@irwinmitchell.com

Contents

Contents

Executive Summary

We're living in a time when data increasingly rules our personal and business lives.

From now until 2025, worldwide data will grow by 61% to 175 zettabytes (one thousand trillion megabytes), according to analysts IDC.

Executive Summary

The IoT – how machines and devices speak to each other – is expanding fast. The UK government's Made Smarter report says there are around 6.4bn data-communicating objects in the world today. By 2020, this is forecast to explode to around 20bn – about 2.45 devices for every human being on the planet.

Data influences our buying decisions in retail and business, whether we choose to shop online or in a store. It also affects who we follow on social media and mainstream media.

Data tells companies which products are selling. Using algorithms and demand forecasting software that aggregates multiple evidence points, it also tells them what types of products are likely to sell next month and in 12 months. Increasingly, data is revealing to manufacturing companies which machines and employees are performing as expected, or not. This applies to agricultural businesses too, who are using data to gain key live insight into their own production processes.

In manufacturing, smarter data has revealed weak key performance indicators (KPIs) in production.

Critics of data monitoring and covert data harvesting, who may liken this to Big Brother and cite the case of Cambridge Analytica, note that privacy rights must be observed. But we must adjust to the reality that their behaviour and performance is being recorded.

This explosion of data capture also has huge benefits. Clever, solid-state-powered sensors can capture valuable data in extreme or hard-to-access environments, protecting people at work.

This technology has been used to measure climate change, and show the world the number of fires in the Amazon and their environmental impact. In manufacturing, smarter data has revealed weak KPIs in production. This has led to increased employment, as the companies improve shop floor efficiencies, become more competitive, increase sales, and hire more staff in non-production roles.

Key Findings – The Growth of Data and the Law

Intellectual property

Research by the Manufacturing Technologies Association says that each year, millions of pounds in intellectual property (IP) rights is being neglected by the UK's engineering sector because companies don't understand these rights and the IP intrinsic in their designs and processes.

Value

All manufacturing sectors, from agriculture to automotive, stand to gain a double benefit from process digitalisation, providing the data captured is accurate. Machinery and (assembly) cell performance can be visible to all to identify bottlenecks. Hours of time searching for missing paperwork can be saved.

Supply chains: sharing data and opportunities

The whole nature of supply chains and contracting at all tiers of a supply chain is being forced to change to reflect the transparency that more data and data sharing provides. Suppliers adapting to these changes readily are well placed to benefit from the competitive advantage it brings.

The University of Cambridge's Institute for Manufacturing's Practical Impact of Digitalisation report found that most digitalisation implementation projects are still focused within one company, often with a single application. Very few encompass supply chains or networks of companies. The value of achieving digitalisation across supply chains isn't yet being fully exploited.

Cyber security

In 2018, over 40% of global industrial control system computers suffered cyber attacks – increasing for the third consecutive year, according to IT security company Kaspersky.

94% of organisations use sensitive data in cloud, big data, Internet of Things (IoT), containers, mobile and other transformative environments. This is creating new routes of attack for cyber criminals, according to Thales' Data Threat Report 2018.

There are many cyber security guidelines and standards to process. Companies must appoint a cyber security director and become familiar with the appropriate security standards, like those advocated by NIST, CIS, NCSC and ISO27001.

Employment law and data protection law

Employment law has always had an impact on manufacturing practices. Companies want to monitor their staff to check productivity, time wasting and behavioural standards, but the General Data Protection Regulation (GDPR) protects the individual from having their data taken without consent.

Both have legal power, but companies must communicate their intention to monitor staff by having a data protection impact assessment, employee monitoring policy, and privacy notices.

Defining Industrial Data

Depending on the company's activity, a typical medium-sized manufacturing business will host several terabytes (TB, or one thousand gigabytes) of data at any one time. How's all that data categorised and organised for efficient operations and adequate security?

Categories of Industrial Data

Data can be defined by its origin and security level (whether originating within or outside the company, whether public or restricted), by its format or file extension (.doc, .xls, .dwf, etc.), or its business function.

It’s also common to refer to either information technology (IT) that runs business processes, or operational technology (OT) that uses data derived inside factory and machine operations, to measure output and productivity.

At the primary level, information is defined as being either human-generated or machine-generated data. Most IT directors recognise that data comes in two types: structured and unstructured data.

Structured data
This is data organised into a specific formatted storage system, such as a database or spreadsheet. The data is easily retrieved for effective processing and analysis. This can be both human-generated and machine-generated data.

Unstructured data
Data that isn’t stored in a predefined format or data model, such as office documents, PDFs, CADs etc. Unstructured data is typically text or image-heavy and human-generated.

"IT data would be a mix of both types, but OT would typically be machine-generated and structured data, although this would depend on how the OT system was coded,” says Graham Thomson, chief information security officer. “It’s possible that OT systems could churn out unstructured data that’s hard to read by other systems".

Information classification

If categorised by security level, ‘information classification’ is the grading of data on its sensitivity or impact to the business if lost or mishandled. It sets the handling requirements for access by people and systems, accordingly, regardless of what type of data or format it is.

Information classifications are often loosely based on military models, which have gained the most expertise in data security. For example, levels may go from ‘PUBLIC’ or ‘INTERNAL’ to ‘CONFIDENTIAL/SECRET’ or ‘RESTRICTED’, etc. An external email from a defence company is often labelled PUBLIC.

> Organisations with good security would normally have an information classification policy that explains the levels and protections required.
>
> They may have examples to make this clear, such as ‘all HR data relating to staff is confidential’, or ‘all engineering drawings are secret,’ and so on.

Graham Thomson
Chief Information Security Officer
graham.thomson@irwinmitchell.com

Data by business function

For business and descriptive purposes, company data is most commonly categorised by business function, whether generated within or from outside the company.

For most manufacturing companies, this matches the functions served by an enterprise resource planning (ERP) system:

- Accounts – including financial operations and regulatory compliance
- Corporate performance, governance and communication – external and internal email
- Customer services – including customer relationships information
- Distribution – including supplier information, warehouse processes and deliveries
- Human resource – including employee database and recruitment
- Procurement
- Sales – including order placement, order scheduling, shipping and invoicing.

Then:

- Production, within which there might be manufacturing
- Engineering – drawings, CAD and technical schematics.

Other levels include:

- Enterprise asset management and business intelligence.

ERP systems have evolved hugely from the basic materials requirements planning (MRP) tools of the 1970s.

Innovations like software as a service (SaaS) make highly expensive ERP available as a monthly service, while the augmentation of ERP offers newer, deeper functions like business intelligence. Modern manufacturing execution systems also provide factory managers and operators with more granular information about their machines, bottlenecks and operator performance.

Information technology and operational technology

What's the difference between a digital enterprise, an Industry 4.0 enterprise, and a modern company today that uses lots of digital technology?

Perhaps the biggest feature of digital transformation is the convergence of information technology (IT) and operational technology (OT).

Historically, IT and OT have lived separately, with limited ability to connect OT data to IT systems. Recent attempts to improve this connectivity, plus big data and the expansion of the Internet of Things (IoT), have created more intelligent manufacturing technology which is bringing IT and OT together.

Drivers of digital integration

The drivers for this convergence are productivity gains and the need for businesses to see their operational data – their fluid volumes, their bulk material yields per batch, machine tool performance, and energy consumption levels – as quickly and as accessibly as their emails and financial statements. IT and OT data for the large, digitally-conversant manufacturer has become unified and accessible across the organisation, from back office to supply chain management to manufacturing operations.

The uniformity provides better visibility of the whole enterprise. Analysts IDC say that 35% of large global manufacturers with 'smart manufacturing' initiatives will integrate IT and OT systems in 2019 to achieve advantages in efficiency and response time.

Some of the terms we associate with Industry 4.0 are realised only when IT is connected to OT. New or better capabilities, such as process optimisation, predictive maintenance, asset management and data-driven decision-making, can be affected when IT and OT are brought together.

For years, manufacturing has invested in employee engagement and change management, bringing employees closer to the goals of the business through better communication. Converging OT and IT helps with this, as production metrics are conveyed immediately to head office.

If it reciprocates well, performance and financials of the company can be shared with employees. Better communication doesn't need a 'cyber physical system', but aligning people, process, data, and tools better allows businesses to achieve higher performance and deliver more profitable production.

Functions of information and operational technology convergence

Technology such as business integration tools (e.g. API integration and Logic Apps), and Enterprise IT, like SQL servers and Azure/Oracle stacks, now help OT communicate more seamlessly with enterprise business processes like ERP, PLM, CRM and MES. Using the IoT, this integrates all the company's technology so managers see factory and energy KPIs as readily as email and financial statements.

Business processes including product engineering	
IT	
Email	Personal devices
Communication, telephones	Collaboration
Enterprise resource planning	Business intelligence, big data
Storage	Databases (e.g. SQL)
Security, sites and content	Cloud infrastructure
Mobility, apps	Networks

Plant management and operation	
OT	
Production planning	Factory automation
Monitoring and controlling systems	Machinery, equipment
Personal identification	Warehouse management
Energy management, smart meters	Smart buildings, smart factories
PLCs	HMIs
Logistics	Yield optimisation

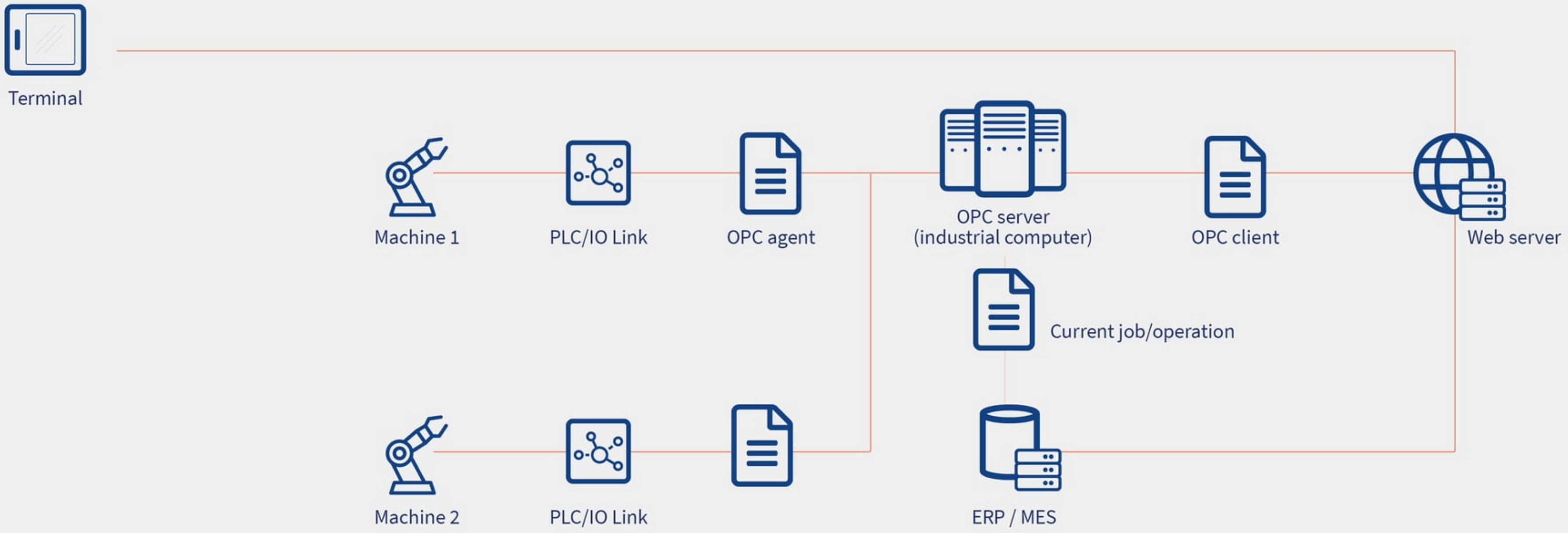
How converging IT and OT creates risk

Where a production system has end-to-end connectivity, cyber security becomes much more than just securing your email and the online activity of your staff. Firms don't always appreciate that a new OT installation, connected to their IT, can breach the security cordon.

“They don't necessarily know the security risk introduced by installing a new machine or temperature control system, which can be accessed by the internet,” says Graham Thomson, chief information security officer. “It can be accessed simply by a commonly-known password if not set up securely.”

As merging OT and IT creates more cyber attack surfaces, companies need to tighten up their security measures.

Factory Automation
Requirements



Terminal

Machine 1

PLC/IO Link

OPC agent

OPC server
(industrial computer)

OPC client

Web server

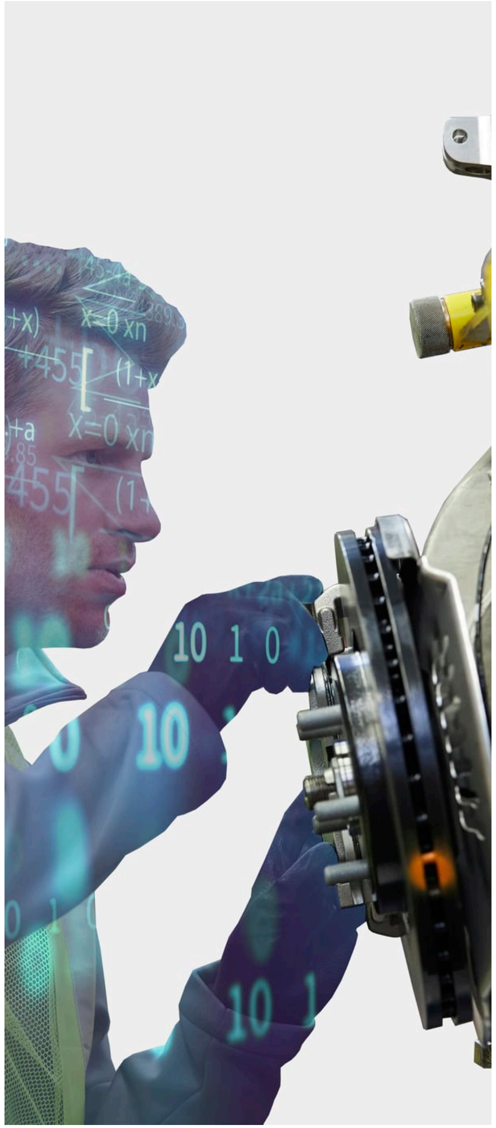
Current job/operation

Machine 2

PLC/IO Link

ERP / MES

Graphic based on Lynq's Your business. Connected. presentation



Manufacturing execution systems

The subject of Industry 4.0 and digital factories, with its list of sophisticated buzzwords and terms, still carries some mystery. But while cyber physical systems exist and autonomous factories are being developed, a factory can be "smart" simply if it tells people what they need to know for correct decision-making.

To do this, hardware and software must combine to collect the right information and display it accurately and quickly to the right people – operators, as well as management.

The pathway of data from the machine to the sales invoice
Machines and factories are connected to enterprise resource planning (ERP) systems to facilitate and assist business decision-making. The connected factory advantage is better appreciated after understanding the pathway that data takes through a manufacturing company.

Say the business is a precision engineering company that cuts and forms metal parts. Sensors in machine tools sense the objective reality of the metal part (such as temperature, proximity, pressure, optical changes, speed, etc.) to detect when it's formed.

Sensors can be electronic or mechanical. A transducer converts the sensed information into an electrical signal, which could be digital or analogue. The data is conveyed to a programmable logic controller, a type of input/output (I/O) device.

Danylo Prokopiv is Chief Product Officer at Lynq, an author of manufacturing execution systems (MES) software. “The digitalisation may happen on the sensor or in a PLC or I/O device, normally installed on the machine,” says Danylo. “The PLC receives data from the machine and converts it to a digital form, then it’s capable of exporting this data into other compatible systems. The data represents an ‘object state’ in time – for example 20 seconds into the milling operation, pressure is 20kPa.”

The next stage can be described as the ‘connected factory’ element. An open platform communications (OPC) server receives the PLC device’s digitised data via an OPC agent. The OPC server is an industrial computer that acts like a printer driver, converting this data to an international protocol language for the ERP or MES systems.

“This OPC server is the stage that gives the factory industrial connectivity, linking the machines to the enterprise software,” says Danylo. It can also buffer the data, retaining it if the network signal is lost. Lynq’s factory software has OPC servers, or drivers, for over 140 types of PLC I/O devices, making it work with almost any factory network.

The data is now exposed to Lynq’s main product, the manufacturing execution system. Factory data can pass from the OPC server directly into an ERP system to be processed for higher, enterprise-level operations like resource management, dispatching, tracking and sales processing.

But using an MES stage like Lynq provides more meaning to shop floor operatives, allowing them to plan and schedule work around the productivity of individual machines and factory cells. This is very useful when demand can spike, and when the variety of product is wide and order volumes are varied.

Communication

Industry 4.0 practices are allowing data to be captured and delivered faster than ever. Manufacturers can enjoy great advantages as a result – but they also need to be aware of the risks.

Data and Employment Law

As digitalisation increases and enhances the analysis of people and processes, two branches of the law are being brought into conflict: employment law and data protection law.

With more data being captured at the point of the machine or the workstation, data will be used in redundancy selection, and performance management exercises. Glenn Hayes is a partner and expert in employment law. He says: “For companies looking to make cost reductions, it’s logical to use this data in redundancy selection and performance management exercises.”

Workstation performance data is just one of the criteria companies will consider – others include attendance and length of service. But machine performance data is objective and not subjective, making it compelling to use in court or tribunal. “Particularly when grading your performance for a redundancy selection exercise, the more objective I can be, the more likely any outcome or dismissal will be fair,” says Glenn.

Glenn Hayes
Partner and employment law expert
glenn.hayes@irwinmitchell.com

Joanne Bone
Partner and data protection expert
joanne.bone@irwinmitchell.com

Data protection rights protect the employee by placing restrictions on how employers use this data. Taking data that relates to an employee, such as their productivity, without their knowledge and using it in an unexpected way to give the employer an advantage is a breach of GDPR. Employers can face huge fines, and must be rigorous in their risk assessments and transparency to avoid this.

“Companies can use data to monitor staff performance, but it has to be transparent to people that you’re using it for that purpose,” says Joanne Bone, partner and data protection expert. The measurement must be legal, proportionate and transparent (via a privacy notice and monitoring policy) to comply with GDPR.

While data alone provides useful evidence to parties in a dispute, human interaction is required to understand the full context of what that data is showing. For example, data alone won’t account for a disability, age, machine defects, or other mitigating reasons for sub-optimal performance.

“If an employee is 65 and is recorded with slower productivity, are they operating the machine slower because of their age, or their ability, or some defect with that machine?” says Glenn. “It’s unlawful to treat someone unfavourably because of a characteristic protected by discrimination laws. Employers have a duty to make reasonable adjustments for disabled employees, so employers need to ask ‘is that discriminatory, and will the company have to make adjustments?’”

A wide selection of hardware and software technology is now available to monitor personnel performance, including CCTV, telematics for drivers, workstation monitoring, and recordings. None of these are barred from use in companies; rather it’s the necessary signposting that’s easy to miss.

“It’s a question of proportionality, risk assessment and transparency rather than being unable to use this type of technology,” says Joanne. “Many manufacturers miss the fact there are preliminary steps, rush ahead and install screen monitoring, CCTV, tracking telematics etc. without working through the issues to ensure that it’s legal.”

If a company is collecting data about a person at work, from a data protection point of view it must tell them what it’s collating the evidence for and stick to that.

Covert recording and filming employees

Knowledge of GDPR is empowering the workforce. There's a rise in the number of cases where employees provide covertly recorded discussions as mitigating evidence in employment tribunals.

A recent Irwin Mitchell case tested whether the act of concealing the recording was an example of gross misconduct. The case ruled that it wasn't automatically deemed an act of gross misconduct, but if people are covertly recording private conversations, it could be judged as such in specific cases.

Filming people in the workplace with their knowledge is becoming more common, as companies trying to improve their process flow and record staff movements between workstations. They can then redesign the factory more efficiently.

CCTV could also flag inadvertent or deliberate time-wasting or other misconduct. This poses the question of whether it could lead to dismissal. Would that be fair?

Litigation trend

Data protection issues are being brought into employment claims more and more. "Employees are leveraging their data protection rights to force a settlement – they know that dealing with a subject access request is potentially time consuming and expensive, and use this fact to try and get a settlement," says Joanne.

It's not just employment cases. In one matter where Irwin Mitchell acted for a consumer business, a buyer was unhappy with the product. When the business said it wasn't at fault, the customer made a subject access request as it'd be expensive to deal with, and threatened to complain to the Information Commissioner's Office, as well to trying to force a settlement.

This performance monitoring could help to accelerate falling employment in manufacturing, as data identifies the weakest piece in the production system.

Best practice guide to data collection notification

Irwin Mitchell recommends that you:

1. Complete a Data Protection Impact Assessment, a form of risk assessment, to make sure you're recording the data proportionately
2. When you're satisfied this is proportionate, assess if the information is transparent enough. Draw up an Employee Monitoring Policy
3. Provide a privacy notice, explaining to the staff again what you intend to do and how the data is collected.

British Airways – first landmark fine for GDPR breach

Employers want to be able to use people's data, but they could face a very big fine if they get it wrong. Fines are huge, up to €20m or 4% of global revenue, whichever is greater.

In July 2019, British Airways was fined £183m for breaching GDPR. It was regarded as a landmark case because it was the first very large fine in the UK since the legislation was introduced in May 2018. BA's breach is an example of third party compromise: the company allowed advertisers on their website, who were then hacked. When customers visited the BA website, personal information was conveyed to criminals without customers' knowledge.

Before the BA fine, just paying the fine may have been the strategy for some companies, as it was perceived it was more costly to change practices than pay comparatively modest fines. Graham Thomson says: "This was the first substantial corporate fine, and shows the leap of fines from the former maximum £500,000 to £180m, proving that you can't afford to get data protection wrong now."

Data Transfer and the Internet of Things

There's a need to transport and deliver data securely and efficiently, in a sustainable way, across resilient networks.

The IoT is about connecting physical devices such as sensors, vehicles, manufacturing systems, domestic appliances and building infrastructure in the physical world to that of the digital. This helps us to track, monitor and manage them remotely and more efficiently. The technologies available for transmitting the data vary – Wi-Fi, 5G (cellular), Bluetooth, LPWAN (low-power wireless area networks, including LoRa and Sigfox) and more.

Many IoT solutions will need to connect over large distances and use very little power, perhaps running off tiny batteries for years. To make them viable, they need to connect over LPWANs, or use solid-state battery technology to keep going without needing recharging.

The Digital Catapult is a government-supported centre that helps companies to learn about and adopt the right data transfer technology for their application. Alex Gluhak, Head of Technology IoT at the Digital Catapult, says: "Lower-power WAN and 5G are examples of future networks, which enable better connectivity between the physical and digital worlds."

At the Digital Catapult's offices in London, partners including BT, Siemens, PTC, Texas Instruments, IBM, Semtech and Servicenow have installed demonstration cells at the Future Networks Lab, the UK's newest dedicated facility for cutting-edge IoT network technologies. Companies can test how each type of "future network" can be applied to their business and create new revenue streams, such as services from products.

Many IoT solutions will need to connect over large distances and use very little power.

Case study: Semtech and LoRa

Semtech is a leading US supplier of high-performance analogue and mixed-signal semiconductors and advanced algorithms. Jeff Gutierrez, Vice President and General Counsel at Semtech, explains how the company's LoRa long-distance, low-power technology fits into the IoT.

What is LoRa?

Semtech's LoRa is a wireless radio frequency technology for use in long-range, low-power networks (LPWANs). The LoRa technology is contained in chipset-integrated circuits. Semtech manufactures the chipsets that are embedded in sensors manufactured by other companies involved in the IoT ecosystem. The sensors collect data that's communicated through gateways to the cloud, are analysed and transmitted to mobile devices such as smartphones or computers.

LoRa devices can communicate over vast ranges using very low power, often far further than Bluetooth or Wi-Fi. A protocol called LoRaWAN creates flexible, large-scale IoT networks.

These IoT networks can operate in any environment, from dense cities to vast rural agricultural areas.

Which is the most widely used LoRa application at the moment? How do you think this will change?

LoRa has shown promise in nearly every field in which it's been applied. A good example of a successful IoT application can be found in smart metering.

Smart utility meters with LoRa chipsets can monitor and collect data on utility usage in real time. This data can be made available to the property manager, allowing changes to be made for more efficient or sustainable energy consumption. Instead of employing the inefficient, time-consuming traditional method of manually inspecting each meter, utility providers can monitor and determine usage rates remotely and cost-effectively with the LoRa technology.

The smart meter industry is predicted to boom in the next few years, and surpass the $2bn mark in 2020. LoRa technology is already available in 100 countries with 100 network operators.

How can LoRa support and be applied to manufacturing businesses?

LoRa can support manufacturing in many ways. Devices equipped with LoRa technology can be used to monitor machine use and temperature to predict when maintenance will be necessary, preventing machine breakdown. Another example is in the smart tracking of assets in or around industrial areas. LoRa makes it possible to monitor assets over a distance of 30 miles from a single gateway.

Have there been some legal issues that your business has faced during its recent growth? If so, what have they been?

GDPR has brought about new challenges for the handling, storage, and processing of data on IoT networks. Its requirements of 'privacy by design' and 'privacy by default' must be considered and applied to the development of IoT networks, products, and services.

Wi-Fi 6 in the Industrial Enterprise

Mettis Aerospace is a global designer and manufacturer of precision-forged, machined and sub-assembled components, primarily in the aerospace and defence markets.

The company occupies a 28-acre site with integrated business units in Redditch, Worcestershire. It employs 540 people and has 3,600 assets or items of equipment on site. It's a technology and development-led business.

Making Mettis digital

Mettis is transforming into a digital factory, taking a lead in digital applications for the forging industry.

As part of the company's Industry 4.0 programme, it's introduced new business systems, automated production lines, and is experimenting with new production technologies. Mettis has partnered with the Wireless Broadband Alliance (WBA) to conduct the world's first Wi-Fi 6 Industrial Enterprise and IoT trial.

Wi-Fi 6 is the next generation of Wi-Fi. It'll have increased capacity, higher data rates, lower latency (response time delays), and will perform better in environments which have many connected devices. The industrial trial, part of a global programme managed by WBA, will enable the use of augmented reality, real-time monitoring of equipment and a host of other applications in an enterprise network environment that'll enable the business to digitise its production lines further.

Mettis's digital factory plan is to:

- Connect everything, everywhere
- Sync business systems with the shop floor, enabling real-time decision making
- Optimise equipment performance using data metrics
- Enhance automation and maximise lights-out capability
- Align work in progress (WIP) with machine data
- Manufacture "golden batches" – data used to repeat perfect delivery.

Examples of WBA use cases at Mettis Aerospace

Use Case 1

Live video feed from press manipulator to control cab

Use Case 2

Real-time energy monitoring

Use Case 3

Machine sensors 12,000t press:
Vibration
Rotation
Liquid levels
Voltage
Valves

Use Case 4

Mixed reality and augmented reality

Benefits of Wi-Fi 6 technology include:

- Higher data rates
- Increased capacity
- Performance in environments with many connected devices
- Improved power efficiency.

Mettis has a highly integrated factory that provides full-service manufacturing, from design to finishing and testing, with forging, machining and other processes in the centre. Mettis uses a visual management system for managing productivity every day, through every centre, at every level. Production schedules are dynamic, and an increase in the right types of data would help them be even more responsive.

A good example of applying Wi-Fi 6 here is video monitoring. Several Mettis presses use video feeds to help monitor accurate operations. Its dynamic drive pool (DDP) press uses real-time video to check and control the manipulator arm.

“Using a camera with a WiFi-6 connection enables a more flexible approach to camera positioning,” says the WBA’s Sarah Markham. “In these environments, having hard-wired connections can be difficult, so doing this with Wi-Fi is a good application. It also needs to have low latency to ensure the video feed is in real-time.”

The Wireless Broadband Alliance – Wi-Fi 6 trials

The Wireless Broadband Alliance is an industry association formed to promote interoperability between operators in the Wi-Fi industry, with the aim of providing an excellent user experience.

The alliance is running several Wi-Fi 6 trials across Europe, and selected Mettis Aerospace as the industrial trial in the UK.

“After the initial trial, Mettis’ grand vision is to install at least 20,000 individual sensors across the business to assist with performance monitoring and predictive maintenance in real-time,” says Bruno Tomas, the WBA’s director PMO.

WiFi-6 is a better technology to deploy in factories with this future-state in mind, Bruno says, rather than trying to make several existing IoT solutions such as Sigfox or narrow-band IoT do what they aren’t designed specifically for.

Mettis’s factory will provide an excellent testing ground for Wi-Fi 6. It’s challenging from a connectivity perspective – there’s a large geography to be covered and industrial radio interference can disrupt signals.

Value

Digitalisation needs a business case. Experts often say there's no point in businesses digitising their processes and capturing gigabytes of data if they can't gain value from it.

Finding Value in Harnessing Data

The government’s Made Smarter Review found that the positive impact of faster innovation and adoption of so-called ‘industrial digital technologies’ could be worth as much as £455bn for manufacturing over the next decade.

Recent research by the Institute for Manufacturing at the University of Cambridge shows that, with some variation, other countries also expect similarly large benefits. Germany has predicted that €425bn will be added from digitalisation in a similar period.

There are clear advantages to transferring accurate information from a paper record or even a spreadsheet to a shared digital place, integrated within the whole business. It provides instant visibility, across the company, where multiple users see the change simultaneously. The information isn’t left or lost on a scrap of paper. Access can be authorised.

This principle hasn’t changed since material requirements planning (MRP) systems first arrived in the mid-1960s. Today, paperless digitised factories are becoming the norm and the digital operating platforms are slicker. Workstation touch screens, tablets, virtual reality headsets – even ‘smart gloves’ – are becoming commonplace.

Taking 2,500 paper documents off the shop floor into a digital format saved tens of thousands of pounds.

Research centres that form the High Value Manufacturing Catapult demonstrate new digital and manufacturing technology to industry. But increasingly they’re being asked for evidence that this smart tech delivers on the bottom line.

“Companies visiting the Advanced Manufacturing Research Centre (AMRC) are impressed with the high-tech machines, but increasingly ask to see case studies with real numbers, showing the demonstrator delivers return on investment,” says Jonathan Bray, Deputy Head of Digital at the Advanced Manufacturing Research Centre with Boeing.

Jonathan has worked for companies including the former European Aeronautic Defence and Space Company (EADS), Airbus and Bombardier. Finding savings in manufacturing processes was a common theme in all these factories, and his job was to apply digital technology to this.

Digitising “kaizen”

Sometimes the digital intervention is most effective (i.e. it reveals the most value) when applied to a simple exercise. A simple “kaizen” (continuous improvement) shop floor movement analysis reveals employee movements and non-value activities.

When working for Strata Manufacturing PJSC in Abu Dhabi, Jonathan calculated the number of times people walked around the shop floor, both necessarily and redundantly. Often wasted movements were to search for paper and flipboard records, time logs, machinery performance and production orders. Digital tablets were deployed to remove paper documents.

“At Strata we took 2,500 paper documents off the shop floor, savings that were easy for the finance and management teams to see. But the greater benefit was from reducing the redundant searches for people and missing paperwork. People were using scissor lifts to search for a paper record out of view, and trying to find engineers to relay information.”

Other unexpected benefits were revealed. The exercise allowed quality inspectors to have their data at the assembly for inspection, as well as digital capturing and reporting any non-conformances identified on parts. Live reporting of issues to engineers removed the need to search for those people.

“Not only did it allow managers to measure and display the metrics to live data, but it gave digital records of engineering response times that previously caused non-conformances against procedural documents, as tracking was via multiple spreadsheets," says Jonathan. “Including digital devices as a single point solution to save paper and manual configuration control demonstrated value upstream and downstream of that solution.”

This might be called ‘digital lean’ – digitising the principles of lean manufacturing (derived originally from the Toyota Production System), removing waste and giving the operator his/her tools at the point of use.

“Businesses tend to see new technology as a single point solution – we’ll buy machine X to fix problem Y,” says Jonathan. “You need to look at what benefits can be made upstream and downstream of that point solution, and involve the people working in those processes.”

How much can companies save by going digital?

Jonathan’s kaizen project saved just over one hour a day per employee in the factory. At a £25 per hour salary with 20 factory staff, that’s a saving of £80,000 a month.

Digital enables services from products

Technology demonstrators can produce new business models and revenue streams. An example is robot suppliers providing a service, with the customer paying for uptime of the robot or the number of holes drilled per week, rather than buying the asset. Downtime of the servitised asset is seen as a penalty, like with availability contracts of aero-engines or trains. This moves the risk of ownership to the vendor, but also guarantees them an income.

While data can save money, realise intellectual property (value), and create new revenues, it can be a liability. For one member, the AMRC analysed data in a manual process and automated it to an artificial intelligence (AI) vision system. This achieved good process improvements for the supplier, but they're now recording more data and have to store it digitally. That can be several gigabytes for each component, so storage becomes an issue and a cost.

"With more intellectual property accessible, the risk of theft could increase," says Jonathan. "There are some great positives from going digital, with many side benefits, but new problems can arise. Companies must learn about it to exploit it."

> As more data is generated, more is learned from it, and a virtuous circle of data generation, interrogation and process iteration is created. That data, protected globally by either database right, copyright, or whatever other intellectual property right the local legislators have used to recognise and safeguard the value of data, will become an increasingly sought-after commodity. This can be used by its creators for their own operational purposes, but also monetised by licensing.

Alex Newman
Partner and
intellectual property expert
alex.newman@irwinmitchell.com

Helping the Food Industry Go Digital

The process of making anything introduces the risk of error. In food manufacturing, the balance of ingredients could be wrong, the temperature and humidity could be sub-optimal, or the mixing process too quick or vigorous.

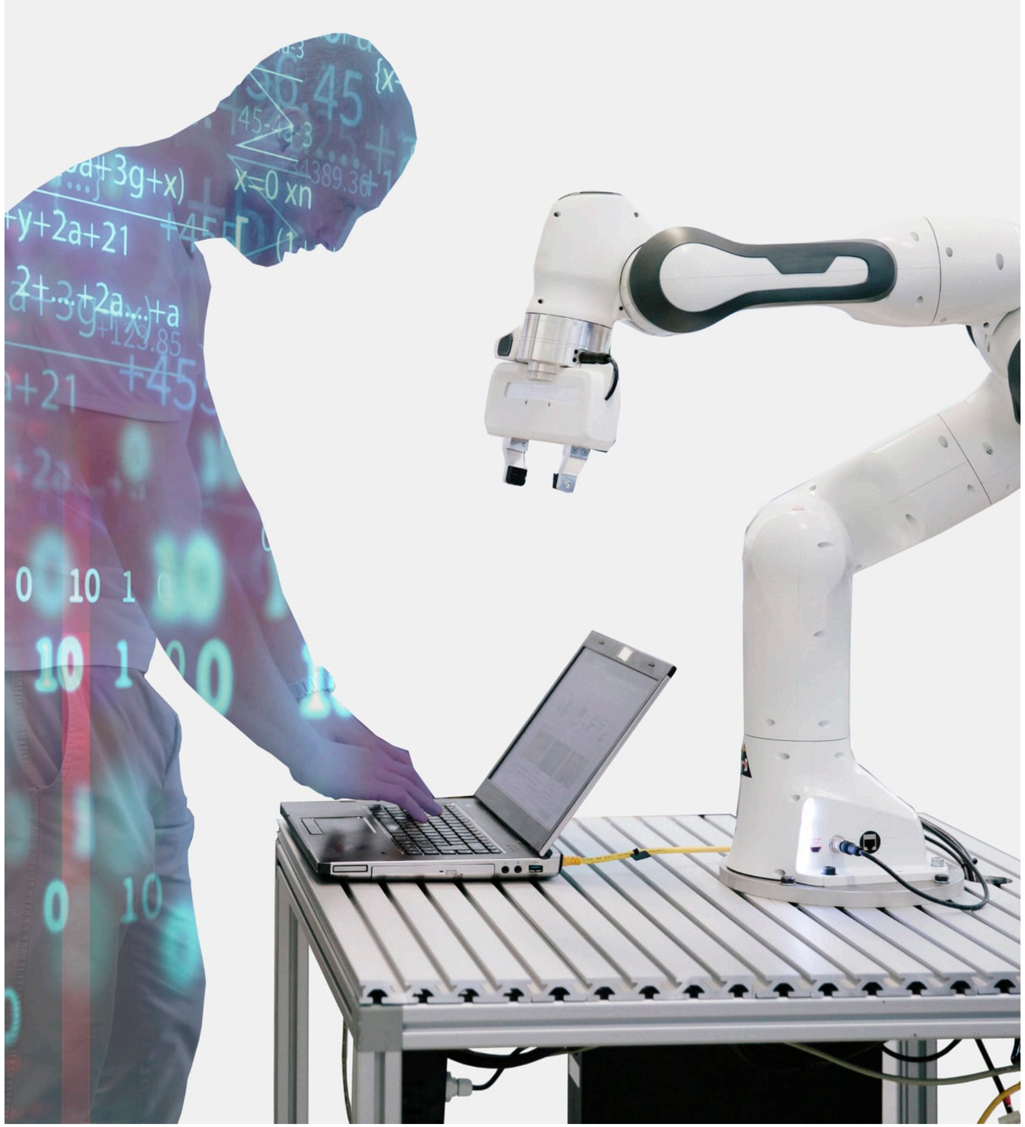
Manufacturers have systems to control these variables, but greater digitalisation is helping them predict and test more situations virtually before they're trialled in production. The food industry is under constant pressure to reduce wastage and improve its sustainability, and digital technology is helping.

Siemens is working with Unilever's research and development (R&D) department to simulate changes to food formulations offline. Unilever's R&D now uses digital twins, including computational fluid dynamics, to test the performance of viscous food mixes, like sauces, before they're manufactured.

"Historically R&D would work on a physical solution, then pass it to production," says Keith Thornhill, Head of Food & Beverage at Siemens. "But only then, when you're committed with a line of machines, can you see some of the problems the mix causes in different conditions."

Faster new product introduction (NPI) and rapid scale-up in a race to get product to market quicker are the drivers for this virtual R&D. Speaking at Siemens' Digital Talks 2019 – Transforming Industry Together event in June 2019, Jonathan Hague, Unilever vice-president R&D Homecare, said that under the traditional R&D regime, a new product often reached the market later than anticipated. Evolving consumer and retail pressures are demanding greater agility, so speed to market is more important today.

Keith Thornhill
Head of Food & Beverage, Siemens



Digital twin modelling gives a more accurate understanding of how equipment will run in a virtual environment.

The pressures come from a highly competitive food industry, and a changing market where the customer knows they have more choice and power than ever before. “The pressure is on to reduce the NPI cycle, and digital R&D is giving us great results,” says Keith.

The food and beverage industry tends to be a follower of production innovation, more than a leader, according to Keith. Low margins in food production create a culture of make-do-and-mend, and this deters capital expenditure spending unless a quick return can be proven.

Digital tools and new business models are helping to de-risk investments. Digital twin modelling of production lines and processes gives a more accurate understanding of how the equipment will run in a virtual environment, before the physical machinery is either purchased or arrives. “This is very attractive to both large companies and SMEs as they strive to increase productivity and agility,” says Keith.

This digital process simulation for food is a key feature of the Materials Innovation Factory, a £81m facility and partnership between the University of Liverpool and Unilever, opened in October 2018.

> New business models, like performance contracts and/or leasing technology, could help to alleviate this. But the digitalisation of retail is giving food companies new opportunities and relaxing the stranglehold of the ‘big four’ UK supermarkets.

Digital benefits small food firms too

More data, and better digital practices, will benefit every size of company. The more connected enterprise will increase efficiency in areas like order accuracy and frequency. How that data interacts with production and logistics fulfilment will give the supplier more visibility and security. For SMEs, if the product range changes frequently, a nimble supplier can benefit if it can respond flexibly too.

Short supplier contracts have been the long-term bugbear for food original equipment manufacturers (OEMs) for decades. Food companies large and small are less willing to buy automation and robots to boost productivity because supermarkets could cancel their contract at any time.

“The big four are under pressure from discounters like Aldi and Lidl that have claimed market share, and from disrupters like Amazon that are building an online grocery delivery service,” says Keith. "While this impacts prices for food suppliers, they will increasingly use digital to sell direct, from the farm or SME manufacturer to the consumer, bypassing the retailer. Digital gives SMEs new routes to market.”

Innovative food products that are more personalised to the consumer or play to a buyer’s regional origin will also drive this online business. While basic commodity foods won’t be affected by this mass customisation trend, foods like confectionery, craft beers, niche gin brands, and higher margin products are already building digital relationships with customers.

For example, the BrewDog beer brand with over 131,000 Twitter followers, successfully raised over £1m from more than 118,000 people in its ‘Equity for Punks’ crowdfunding round.

Long-Life Sensors Reduce the Noise

Graeme Purdy
CEO, Ilika

Small, very light, and powered with solid-state cells, Ilika's sensors are enabling condition monitoring and data collection in a wide variety of environments where conventional sensors can't work optimally.

Sensors make the IoT possible. They capture data from assets – consumer, industrial, medical – and convey that data to a computer which analyses it and then connects these outputs to other machines in the network.

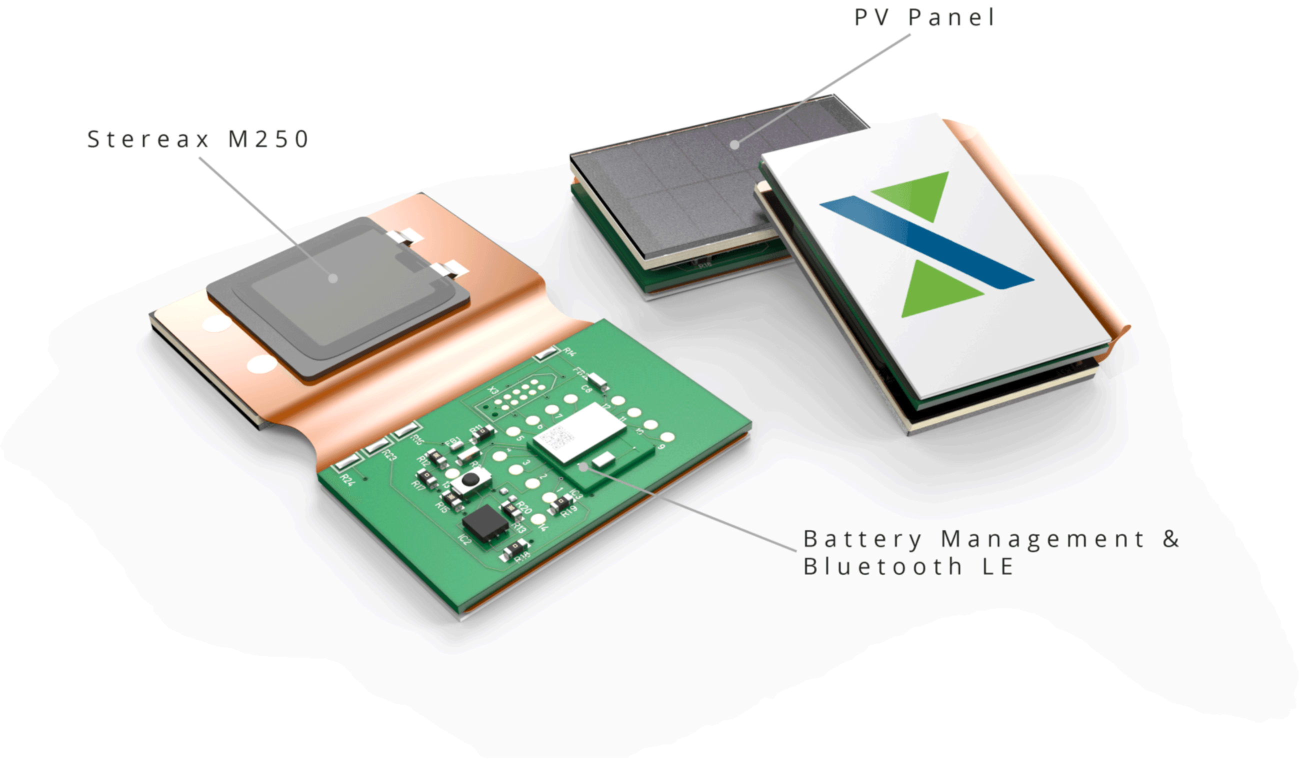
But historically sensors used in IoT, often referred to as 'end nodes', have either been hard-wired to a larger power source, as with mobile phones, or powered by coin cells that have a short lifetime and a big environmental footprint. Using cables limits the type of applications where a sensor can operate, and wireless, battery-powered sensors need to be maintained and replaced. Frequently, the places where these sensors are useful are found in hazardous or hard-to-access places.

Instead, solid-state cells can power these end node sensors more sustainably, over many cycles, usually in combination with an energy harvester, such as a small solar chip that creates an electric current from sunlight.

Ilika designs and develops these solid-state batteries for contract manufacture elsewhere. They can be very small, suitable for embedding in devices, such as wind turbine blades, and in the human body. They last a very long time, typically about 10 years. They're also very suitable for the tough operational conditions encountered in industry: mining, energy, transport, and more.

Ilika has developed its solid-state battery technology with the brand name Stereax. “Instead of having a liquid electrolyte, which makes batteries flammable, these use a solid electrolyte material which makes them a safer, more stable electronics component,” says Graeme Purdy, Ilika’s CEO. “They’re non-flammable and rugged for industrial conditions like high temperatures and pressures.”

The company is growing, as a wider range of applications are identified and exploited. Ilika’s end nodes are used by the rail industry, in wind turbine development, and in medical applications where electrical pulses can replace drugs as an alternative, internal treatment.



Condition monitoring of the national rail network

Helped by grant funding from Innovate UK, an 18-month project with Network Rail will develop, deploy, and test self-powered sensors for monitoring key parameters affecting the performance of the railway infrastructure, covering load, temperature, and shock.

The self-powered sensors will be maintenance-free, and will generate data 24/7, 365 days per year. The solid-state battery powered sensors will be the first of this type developed and tested for the railway industry.

Ilika's sensors are also used in applications including the condition monitoring of wind turbines with Titan Wind Energy, the largest manufacturer of wind turbine products in China. Another use is medical implants with Stereax M50, a small and super-lightweight medical battery inserted in the body to measure blood pressure, glucose levels or even to administer treatment such as insulin pumps.

"Products that were historically passive are being re-engineered and given communication capabilities," Graeme says. "One reason for using these batteries in medical devices is they are biologically inert, and will therefore do no harm. These work as 'biolelectronics,' such as neurostimulators – devices that are replacing the job that drugs conventionally do."

How does the technology cope with the huge volume of data being captured by the IoT? These end nodes function as a capture and transmission device, transmitting the data they capture, sometimes via a mobile phone signal, to the operator's CPU to process. The customer will have sophisticated IT systems, and large data centres or possibly cloud computing, to process the high volumes.

"The challenge for industry is to capture the right type of data that's useful for diagnosing the system," Graeme adds. "Using wireless end nodes, you can position sensors to acquire data that's really relevant to the application, increasing the quality of the data and reducing the 'noise.'"

The sensors will combine the Stereax technology and partner Smart Component Technologies Ltd's Novel ultra-low power sensor platform. They'll be wirelessly connected to Network Rail's existing condition monitoring platform.

Sharing Data in Supply Chains

Sarah Riding
Partner and commercial law expert
sarah.riding@irwinmitchell.com

Businesses have always shared information with their suppliers and customers, but the amount and the categories of data shared vary according to the activity. High-volume and high-speed deliveries dictate that more data is conveyed quickly.

Most industries – certainly defence, nuclear, specialist chemicals, even food – apply confidentiality agreements to the data that passes between parties in a chain to control IPR in such a rapid, seamless exchange.

The digitalisation of business has accelerated the speed and volume of this transmission. Competition, the focus on customers, and greater product customisation are driving this.

Low-volume vehicle manufacturers such as Bentley Motors can now turn out fully customised cars, with hundreds of small permutations making each car unique, at the same rate as they were making just five or six models in a handful of colour schemes 15 years ago. High quality data from the customer order to the shop floor and the suppliers' purchase orders make this possible – as well as a skilled workforce, adaptive manufacturing technology, and good management.

- Data sharing has improved customer-supplier relationships, often leading to long-term contracts and loyalty
- Suppliers have to buy technology and tools to be in a connected supply chain and share their data, imposing costs – but the prize can be great
- Demand forecasting – the ability to source and interpret data from multiple sources (including social media) means companies can respond more quickly to changing trends.

While other sectors don't work to the minute-by-minute drumbeat of volume car manufacturing, most industries now use data in sophisticated ways.

Suppliers today have to be more proactive about the way customers require their information. "Previously a company would enter a supplier contract, and there'd be strict parameters about performance and delivery," says Sarah Riding, partner and commercial law expert. "Now, because everything is real-time, there's more collaboration, visibility, transparency, and a big push on how that data is being used for forecasting and predicting lead times, as well as its flow through the supply chain."

Automotive is the sector best known for 'just-in-time' manufacturing, where parts are delivered to the factory – indeed the correct assembly bay in the factory – within hours or minutes of the order being placed. At Johnson Controls in Sunderland, dashboards show which sequence of neighbour customer Nissan's car models are in production that day. Orders are placed for seats and handbrakes with specific trims and left-hand or right-hand drive cars at the same time they appear in Nissan. In less than an hour, certain just-made components are being shuttled to the giant factory next door.

While other sectors don't work to the minute-by-minute drumbeat of volume car manufacturing, most industries now use data in sophisticated ways to increase order accuracy and reduce delivery times. Aerospace is a good example, and especially important as the rate of aircraft production rises.

The Sharing in Growth programme has helped 63 SME suppliers win big orders from existing and prime aerospace customers by helping them become better suppliers: more training, better leadership and vision, and new investment in technology and processes, including automation. These SMEs wouldn't access these contracts if they couldn't share nearly all their engineering data and processes.

Data is making the customer king

Most participants in this process have had to provide data about their processes, machines, tooling, shift patterns, and other KPIs to the prime customer. This builds trust and solidifies long-term agreements, but some SMEs are cautious that revealing all their data will lose them some niche advantage.

“More confidentiality agreements are being put in place earlier on,” says Sarah. “For small suppliers, being forced to share that information early on is more difficult – this is your intellectual property. Also, you’re being forced into the position to buy certain technology – like software or tooling – to be in that connected supply chain, like an extension of the prime customer.”

But there are advantages, and some suppliers see transparency as a good thing. “Because there’s now a more transparent arrangement with a customer, if they’ve committed to install technology to make something better, they feel they’re more tied in to that customer,” says Sarah. “It’s harder for the customer to break that.”

Another trend is the growth in the range of personalised products. Technology has enabled new product development (NPD) and greater product customisation.

‘Nike By You’ is the sportswear company’s model to allow customers to personalise some footwear models with their own features. A new generation of companies are offering a degree of personalisation to their products, to buy customer loyalty.

Companies must understand privacy laws fully so that the data they’re using to personalise a product is used and stored with the buyer’s consent, and that this is explicit at the product portal.

Security

Manufacturing is the third most likely sector to experience a data breach, after financial services and insurance. But it's among the least protected, according to the manufacturers' organisation Make UK.

Good Cyber Security Practice

Manufacturing is highly vulnerable to cyber attack

- In 2018, over 40% of global industrial control system computers faced a cyber attack, according to research by IT security company Kaspersky, an increase three years running
- 60% of Make UK members have at some time been subject to a cyber security incident, almost a third of them suffering financial loss or disruption to business as a result
- 84% of manufacturers believe greater Industry 4.0 connectivity will increase the risk of cyber security breaches, with 31% saying cyber security isn't taken seriously enough at their business (BDO Digital Transformation report)
- 41% of manufacturers say they've already been asked by a customer to demonstrate or guarantee the robustness of their cyber security processes (Make UK 2019 report)
- 35% consider that cyber vulnerability is inhibiting them from adopting industrial digitalisation technologies fully (Make UK).

Cyber threats are constraining UK industry's progress with digitalisation.

Companies can be hacked, covertly observed, and have their assets damaged or stolen while remaining completely unaware until it's too late.

Because Industry 4.0 technology makes a company more connected to machines, the internet and other companies, firms are wary – with good reason – that high levels of digital adoption will increase their exposure to cyber attack. In a study with cyber security providers Vauban Group, Make UK found that while manufacturers are investing in digital technologies, 35% think that cyber vulnerability is inhibiting them from doing so fully.

Cyber attacks also show how closely integrated business IT (business communications and computing, storage and back-office technology) is with operational technology today. "For Industry 4.0 especially, IT and OT have already converged, and at a speed greater than companies have been able to secure them adequately," says Graham Thomson, chief information security officer. Industrial cyber attacks will increase, Graham says, impacting industry in areas like breaches of security, outages, data and IP theft, physical damage to IT systems and to capital equipment.

Industrial espionage

There are several ways a cyber criminal can attack a manufacturing company, including phishing and other "social engineering" techniques, resulting in malware (virus) infections like ransomware and Trojan horses.

Phishing is the fraudulent attempt to acquire sensitive information like passwords and protected files, or to deploy booby-trapped files, by posing as a trustworthy party. It's the most common form of cyber attack because there's a constant stream of different vulnerabilities that a hacker can take advantage of. It could be elicited through a fake advertisement on social media, or masquerading as an email from a work colleague.

The risk is magnified with such attacks because companies can't always detect the level of security risk being introduced. "Say a company installs a new HVACS [air conditioning] system, but they didn't know this is accessible via the internet," says Graham. "It can be accessed from afar simply with a commonly-known password, if this isn't set up securely.

"A hacker can play with the settings, making conditions too hot or cold to work efficiently, or possibly even use this system to then access other internal IT systems," says Graham. "It's a very effective impact from a simple intervention."

Hacking and modifying a factory operation can be achieved by attacking any management system of operations technology.

Hacking and modifying a factory operation can be achieved by attacking any management system of operations technology, or supervisory control and data acquisition (SCADA) architecture. Most manufacturing companies have a variety of these OT systems to manage their factories inside their corporate IT structure which are also accessible remotely, which is where criminals target.

Normally industrial companies have an 'air gap' between OT and machinery and their IT network, preventing easy access to the plant for cyber criminals. "Regularly we see simple methods like a USB stick breach the air gap," says Graham, "So by itself, partitioning factories from the network with an air gap isn't an effective measure."

Password or credential stuffing

A rising cyber trend that manufacturers should know about is password stuffing.

The login pages for a website, email account, management or control system for operational technology are all at risk from this method.

Cyber criminals can acquire lists of previously compromised email address and password pairings. They run a program to populate login pages with millions of combinations.

“There are about 3bn passwords and usernames on these lists that have been compromised, where numerous security researchers have found these databases on the dark web,” says Graham. “They point the program at the login page, press go, and the combinations auto-populate until there’s a match.”

While the method relies on complete chance, it’s possible to gain unauthorised access using email addresses and passwords that were compromised years ago and are totally unrelated to the current business, where an employee used an identical or commonly-used password. The solution: use two-factor authentication for remote access to important systems, or at the very least enforce long random passwords.

Best practice for cyber security

What does good look like in cyber protection for a manufacturing business?
A common problem is there’s a lot of IT security information and standards, some contrasting, and most people don't know how to get the best information. A good example is the Cyber Essentials Scheme, the government’s basic guidance for business protection. In their 2017/18 cyber survey, Make UK said over 70% of companies hadn’t heard of or applied for this, even though it’s free, and only the basic level of recommended protection.

Improve your cyber security

Graham Thomson, chief information security officer, recommends these steps:

Appoint somebody with sole responsibility for cyber security for the organisation. Provide them with a framework and reporting structure. For SMEs, this may mean combining the job with another role like IT director.

Make security part of the organisation's culture, not just an IT issue. "Being cyber secure covers employees' behaviours, training, and deploying cyber safe processes. Staff need training and better awareness of the risks," Graham says.

Become familiar with the different security standards. Several documents can tell you how to apply good IT security: many are free like NIST and CIS, some like ISO27001 are paid-for. Most are very lengthy, and will need a lawyer to translate appropriately for the business.

Outdated control software not fit to protect against modern threat

Tom Lawton, partner at BDO LLP, highlights cyber security risks and common reasons for breaches from BDO's 2019 Manufacturing Digital Transformation Report.

"Cyber security represents a huge challenge for the manufacturing sector in an era shaped by digital transformation. As technology and greater connectivity transforms the way manufacturers operate and deliver products and services, the potential impact of cyber-attacks grows exponentially. This hyper-connectedness of systems allows attackers to target systems through new routes. Threats include attackers trying to disrupt manufacturing processes, or trying to exploit systems to get their hands on intellectual property.

"When reviewing cyber security frameworks of manufacturing clients, we often come across the following issues:

- Highly complex viruses and malware that use multiple routes and steps to target particular chipsets and known vulnerabilities in industrial process software and firmware
- Lack of appropriate network segregation and potential breaches of the 'air gap' between the manufacturing and corporate network infrastructures
- Industrial control systems that were designed and built for an extended service life, before data networks provided a conduit for cyber threats – these frequently run outdated software that lacks integrated cyber defences and the frequency of updates to counter constantly emerging threats
- A lack of expertise and resources to maintain legacy systems, which leads to both operational and security risks
- No formal allocation of responsibilities for security between IT and engineering departments.

Manufacturers must ensure they have adequate controls in place to deal with these new cyber threats. Appropriate plans need to be put in place in each of the four main areas – prevent, protect, monitor and respond – to address the associated risks."

Tom Lawton
Partner, BDO

Security and the Supply Chain

As large organisations become increasingly data-driven, the data security industry is booming.

Thales is a leader in advanced data security solutions and services. The company's brand message is about providing "digital trust" for device manufacturers and organisations deploying IoT devices. This includes data encryption, device authentication, and firmware signing.

Thales has developed expertise in data security, partly because of the complexity of its core business where data is often siloed. Paul Starbuck, Head of Digital Industry and Methods at Thales UK, says: "We manufacture lots of discrete things but rarely in high volumes – that siloes datasets."

Data management gets complicated in big defence contracts that share sensitive data, from multiple data communication protocols and sources, Paul says. "You have the same inputs and outputs [as other companies] and you run through the same process, under a government standard, but the projects become very separated. Protecting the security of our own very wide product base has helped us perfect a data security and management business for other large customers."

The company helps customers to organise and structure their data so it's compliant, verifiably 'single-source,' visible throughout a supply chain to qualified users and secure. The KPIs of manufacturing haven't changed with digitalisation; managers need to know the yield, the product is on time, it conforms to the regulations, and how much it costs. But today people expect this information quickly, to know the deviations, and how to predict what the risks of non-compliance and delay are immediately.

"Companies must be able to find that data, and provide it to their supply chain in a structured way," says Paul. "How you choose to share it becomes very important in a secure environment." Tools such as product data management (PDM) or product lifecycle management (PLM) software and building information modelling (BIM), which provide a common data platform, are now standard in engineering industries.

Part of the task of the data security provider is to secure all data, but only provide the data needed. "Often suppliers only need one subset of that data – they only to know where the BOM [bill of materials] is or where the drawing is, i.e. the data they will do something with," Paul says.

Organising, tagging and trust

Data needs to be marked for identification, and to apply access preferences for employees and users in a team or supply chain. Thales uses baked-in meta tags behind all of the company’s proprietary data that allows accurate sorting and management.

“This creates a core dataset marked 'All Product Family data', a single large database that employees can login to see what data is available for a project, what’s possible to access and what people are allowed to do with it," says Paul. “It shows what’s shared or is marked with a level of confidentiality, sometimes that we’re unable to share across Thales. We’re working to increase the robustness of this tagging approach – it’s the foundation for data transparency and storage.”

The next stage is the choice of several data security products and services.

These include:

- Data encryption and data in motion encryption
- Product certifications
- Key management
- Authentication and access management
- Tools for mobile and online payment
- Whole solutions such as cloud security.

Industry 4.0 and the cloud

More industrial data is being stored in the cloud and off-premise, but for many companies the idea of an open-source cloud environment is still unnerving.

Thales’s 2018 Data Threat Report says that 94% of organisations measured use sensitive data in cloud, big data, IoT, containers, mobile, and other transformative environments. This change is creating new attack surfaces, and new risks for data that need to be addressed with robust data internet security controls.

Previously, companies ensured there were air gaps between their customers’ secure networks and the Internet to protect their data. But cloud storage still seems very accessible with the correct trust protocol in place. Consequently, cloud solutions like bring your own encryption (BYOE) key management and SaaS security have been developed.

The challenge today is to secure data adequately in a free-flow world, a world that expects Industry 4.0 connectivity with no security downside. When companies understand how to do this, they can sell it as a benefit, a new service.

“This is what we help customers to do – create businesses from controlling, securing and issuing their data securely to partners,” says Paul. “At the outset of Industry 4.0, people didn't appreciate the true value of their data. We’re determined that companies better understand this.”

Industry Demands More Training in Cyber Security

Demand for IT security jobs has increased in recent years. According to the website ITSecurityjobs, the number of these jobs advertised in the last quarter rose by over 50% compared to the same three-month period in 2010.

Salaries have also risen, with the average salary for a permanent IT security job rising by 16% per annum. Contract IT security jobs have also seen a rise, with the average daily rate increasing to £450 – up 6% on last year.

The education sector has responded. More universities have launched cyber security and IT security courses, especially Masters degrees. FindaMasters.com estimates there are 160 such courses in the UK now. Universities that run cyber security degree courses approved by GCHQ, the government intelligence and security organisation, include the University of Oxford, Cranfield University, Edinburgh University, Lancaster University, and the University of York.

Cranfield University: Cyber-Secure Manufacturing MSc

The first cohort of the Cyber-Secure Manufacturing MSc at Cranfield University in Bedfordshire graduated in October 2019. The course was proposed four years ago by Cranfield’s Industrial Advisory Board to address the high career demand in the IoT, big data, cloud computing, and cyber security disciplines.

The course combines Cranfield's established expertise for delivering high-quality Masters programmes in the manufacturing and defence sectors with the need for higher operational IT security personnel from engineering companies, including Atkins, Rolls-Royce, and Airbus.

What the students learn

Dr Konstantinos Salonitis

Cranfield University

The course aims to train students to identify a variety of cyber threats to any cyber physical system in the business that's exposed to the internet or other intrusion. It covers all types of threats that a cyber attacker could use, including phishing, malware, ransomware, and industrial espionage. It also helps students understand the change to the business risk by putting data in the cloud.

Advised on by industry, including visiting lecturers from Atkins plc and BT, the course is built to equip people with good preventative and responsive skills to deal with IT security.

Dr Konstantinos Salonitis is Acting Head of Sustainable Manufacturing Systems Centre, and Reader in Manufacturing Systems at the Sustainable Manufacturing Systems Centre at Cranfield. "For the preventative aspect, we teach the strategies to protect the whole system – both IT and OT – from different types of cyber threat," he says "For the responsive aspect, if there's an incident, what do they need to remove the risk, protect the system immediately, and secure the system from this incident in the future?"

While some programming and knowledge of algorithms is required, the main skills taught are in problem identification, vulnerability assessment, penetration testing, and the correct way to implement remedial processes.

"The aim is to become experts in protecting industrial systems efficiently," says Dr Salonitis. "Also, students learn about assessing the threat levels, and how to identify a malicious attack from a hacker that's interfering with the system non-maliciously."

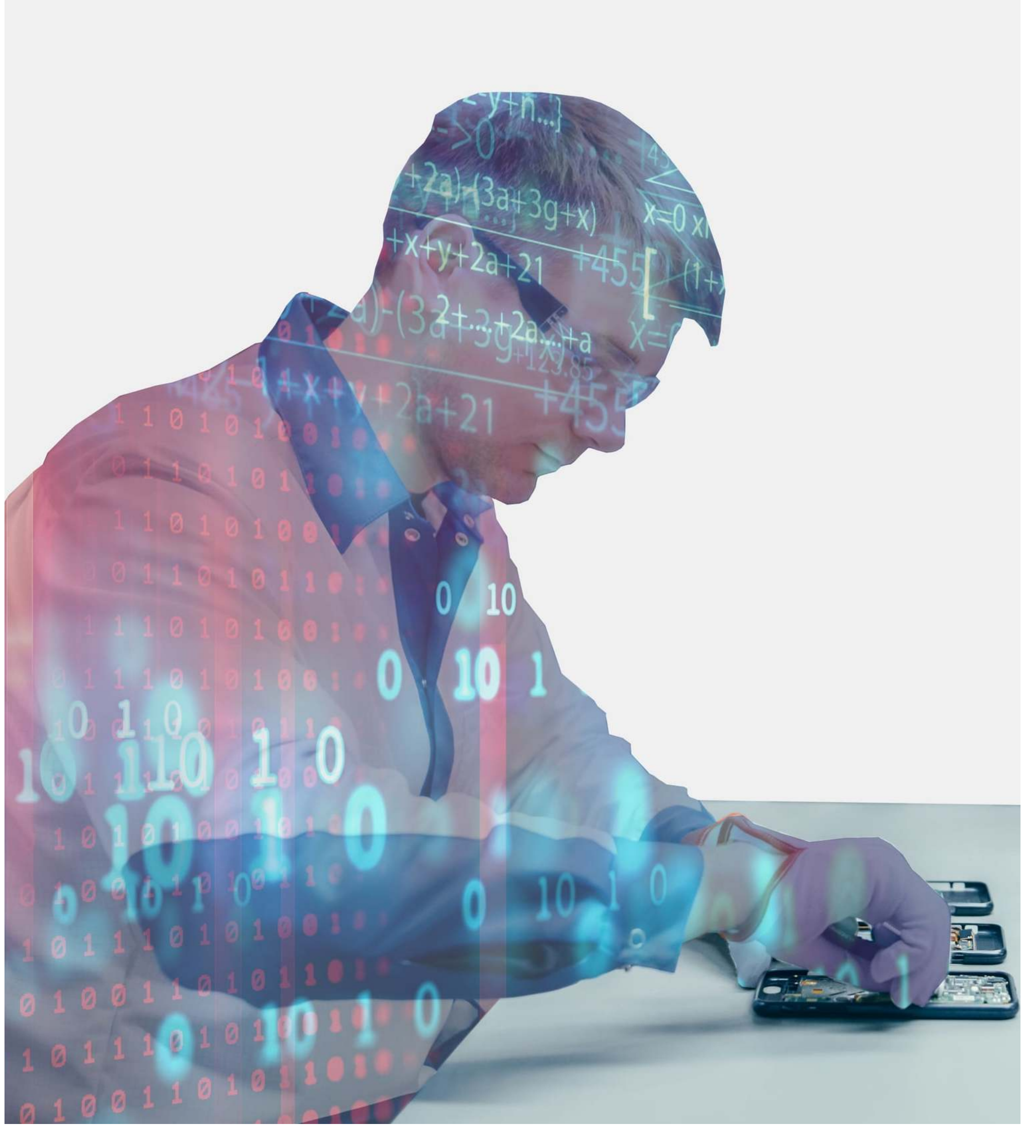
Phishing is the most common type of threat, but ransomware is potentially the most serious and costly. Machines are vulnerable to attack if they're exposed to the internet or a malicious individual.

Dr Salonitis gives the example of an autoclave – an oven for baking composite components – whose temperature is being tampered with remotely. “It’s possible that someone might do this mischievously rather than for ransom or with the intent to sabotage the machine. We provide the knowledge to detect the real motive, which can best protect the system.”

While Cranfield’s industrial partners tend to be in aerospace and defence, cyber security skills are needed in all sectors of manufacturing and business. Graduates of these courses can also help companies that don't need a full-time chief information security officer (CISO), but do need occasional testing and cyber protection assessment consultancy.

The course covers eight modules, a group project (20%) and a three-month individual project (40%). Courses are full-time or part-time, and involve 20-30 students. It addresses the main IT security challenges in smart manufacturing, including the skills to:

- Identify cyber threats in manufacturing systems from cloud
- Protect manufacturing systems from cyber attacks
- Improve incident response and disaster recovery in manufacturing systems
- Assess the cost of cyber security solutions for manufacturing systems.



Glossary

Glossary

This glossary is provided as a reference to the meaning of some of the technical terms used in this report.

Analytics, big data and AI
A suite of intelligent tools – machine learning, cognitive services, data lake analytics, Databricks, Spark – that probe business systems deeper, analyse further and enable systems to "think for themselves."

Asset management (industrial)
A key part of large industrial operations, asset management is the combination of management, financial, economic, engineering, and other practices applied to physical assets, with the objective of providing the best value level of service for the costs involved.

Distributed control system (DCS)
A DCS is a digital automated industrial control system (ICS) that uses geographically distributed control loops throughout a factory, machine or control area. It allows each section of a machine to have its own dedicated controller that runs the operation. A DCS is the building block of the Industrial IoT.

Enterprise business processes
Whole enterprise software systems that help measure and control many levels and facets of a company, system or complex assembly. Examples include CRM, PLM, ERP and MES systems.

Enterprise resource planning (ERP)
Enterprise software linking all departments of the company to provide better holistic visibility of its workings and bottlenecks.

Human machine interface (HMI)
A user interface or dashboard that connects a person to a machine, system or device, most commonly applied to an industrial process. HMI is to OT what the user interface is to IT.

Industrial Internet of Things (IIoT)
A system of interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management.

Information technology (IT)
Top-down technology support for management and administration, based on communicating information.

Machine learning
An application of artificial intelligence (AI) that gives systems the ability to automatically learn and improve from experience without being explicitly programmed.

Manufacturing execution system (MES)
An information system that connects, monitors and controls complex manufacturing systems and data flows on the factory floor. MES helps optimise production by understanding current conditions on the plant.

MTConnect and umati
Manufacturing technical standards or machine interfaces, to retrieve process information from numerically controlled machine tools. Umati is a European machine interface recently introduced by Germany's machinery trade body, VDW.

Open platform communications (OPC) server
Industrial computer that analyses data from the machine via the PLC/IO link. Provides information like good parts, bad parts and machine state.

Operational technology (OT)
The control of processes and changes in processes through the monitoring and control of devices. Examples of OT include automation and robotics, logistics, production planning, asset management and energy management.

Process control
How machines are controlled. Three of the main systems are PLC, DCS and SCADA.

Product lifecycle management (PLM)
An information management system that can integrate data, processes, business systems and people in an extended enterprise. PLM software allows you to manage this information throughout the entire lifecycle of a product

Programmable logic controllers (PLC)
An industrial digital computer that has been adapted for the control of manufacturing processes, such as assembly lines and robotic devices.

PLC/IO Link
Input/Outputs and PLC controllers – data generated by a machine passes through this filter for preparation for processing by an OPC server. It's the link between the machine and the industrial computer before human interpretation.

Supervisory control and data acquisition (SCADA)
An industrial computer system architecture for high-level process management, while using shop floor devices like PLCs and PID controllers to interface with machinery.

Terminal or tablet
A device to display data, often real-time, generated in a factory or business. Data is often fed by an MES or equivalent factory management system.

User experiences
Describes the visual and tactile devices used to convey the meaning of industrial data to a user. Examples are dashboards, mobile devices, and mixed reality.

References

References

The links below are provided for further reading on specific subjects.

Get Yourself Connected

Fourth Industrial Revolution: Beacons of Technology and Innovation in Manufacturing. (2019) World Economic Forum.

Information technology and operational technology

What Is The Difference Between IT And OT? (2019) Coolfire Solutions.

Information Technologies (IT) Vs Operational Technologies (OT). (2019) Randed.

Aruba, Siemens Partner To Accelerate IT, OT Network Convergence. (2018) CRN.

Manufacturing execution systems

Factory Automation Guide. (2019) Lynq.

Data and employment law

Employees who covertly record Meetings. (2019) Daniel Barnett.

Intention to fine British Airways £183.39m under GDPR for data breach. (2019) Information Commissioner's Office.

GDPR – Guidance for Employers. (2017) Irwin Mitchell.

FAQs: GDPR and HR. (2017) Irwin Mitchell.

Wi-Fi 6 in the industrial enterprise

Wireless Broadband Alliance. (2019)

The Wireless Broadband Alliance And Mettis Aerospace Announce World's First Wi-Fi 6 Industrial Trial. (2019) Mettis Aerospace.

TP-Link. (2019)

Finding value in harnessing data

Made Smarter. (2017) UK Government.

The practical impact of digital manufacturing: results from recent international experience. (2018) University of Cambridge.

Helping the food industry go digital

Digital Talks 2019 – Transforming Industry Together. (2019) Siemens.

Jonathan Hague of Unilever speaking at Digital Talks 2019. (2019) youtube.com.

Good cyber security practice

Cyber Security and Manufacturing – A briefing for manufacturers. (2019) Make UK.

Stuxnet: the father of cyber-kinetic weapons. (2018) CSO Online.

10 steps to cyber security. (2019) National Cyber Security Centre.

Computer Security Resource Center. (2019) National Institute of Standards and Technology.

CIS Controls. (2019) Centre for Internet Security.

ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT. (2019) International Standards Organisation.

Security and the supply chain

Thales. (2019)

Keeping businesses and organisations cyber secure. (2019) Thales Group.

2018 Thales Data Threat Report European Edition. (2018) Thales.

Other useful references

Manufacturing; Digital Transformation Report. (2019) BDO.

IDC: Expect 175 zettabytes of data worldwide by 2025. (2018) Network World.

What is Manufacturing Execution Systems (MES)? (2018) youtube.com

umati: universal machine tool interface. (2019) VDW.

Engineering sector losing millions by failing to protect IP like creative industries, MTA survey shows. (2017) Manufacturing Technologies Association.

Hackmageddon. (2019)

Pwned websites. (2019) haveibeenpwned.com.
List of data breaches and cyber attacks in May 2019 – 1.39 billion records leaked. (2019) IT Governance.

2019 Internet Security Threat Report. (2019) Symantec.

Credits

A report for Irwin Mitchell by:

stirlingmedia

with thanks to:

LYNQ

SEMTECH

CATAPULT Digital

METTIS AEROSPACE

ilika

AMRC ADVANCED MANUFACTURING RESEARCH CENTRE / The University Of Sheffield.

BDO

SIEMENS

THALES

Cranfield University

All images reproduced with permission

Thank you for reading

Going Fourth