A clear and present danger to manufacturing

In conversation with Bill Ruh, CEO GE Digital

Why partnerships are the key to smart factories

Becoming early adopters of pioneering brands
WORLD CONGRESS

BARCELONA
16-18 OCTOBER 2018

THE LEADING IOT INDUSTRY EVENT

CONNECTED TRANSPORT
MANUFACTURING
HEALTHCARE
ENERGY AND UTILITIES

BUILDINGS & INFRASTRUCTURE
OPEN INDUSTRY
ENABLING IOT

TWO CO-LOCATED EVENTS:

IN PARTNERSHIP WITH:
ON THE COVER

32 CYBERSECURITY
Clear and present danger

16 THE CTS INTERVIEW
Bill Ruh, CEO of GE Digital

60 SMART FACTORIES
Why collaboration is key

54 IT INNOVATION
Risk and reward

NEWS & ANALYSIS

02 News
Gartner says global artificial intelligence business value to reach $1.2 trillion in 2018

03 News
Existing IAM solutions are creating major barriers to digital technology adoption

04 News
Robots a welcome addition to the workforce

05 News
IoT, robotics and machine learning set to transform the supply chain

06 Comment
Jason Chester, director of global channel programmes, InfinityQS

07 Comment
Neil Bosworth, UK manager, Gemalto M2M

08 Comment
Mark Homer, vice president global customer transformation at ServiceMax from GE Digital

08 Comment
Sam O’Meara, UK director, Applause

10 Analysis
Dealing with disruption

10 Analysis
Pointing the way to IIoT success

64 Final Word
Leading the way in Industry 4.0

THE CTS INTERVIEW

16 Bill Ruh, CEO of GE Digital

SPECIAL REPORT: CYBERSECURITY

28 A rising threat

32 Clear and present danger

35 Passwords are not going away

36 The five stages of cloud security

FEATURES

20 Augmented Reality
Dawn of a new reality

38 Real-Time Insights
The critical path to manufacturing efficiency

40 Disruptive Technology
Roadblocks for 3D printing

44 Factory Automations
Bottle Job

48 Smart Meetings
The expanding workplace

50 Wide Area Networks
Blended Connectivity

54 IT Innovation
Risk and reward

56 Real-Time Data
Risk and reward

60 Smart Factories
Why collaboration is key

62 Edge Computing
Living on the edge

www.connectedtechnolgysolutions.co.uk | 01
Gartner says global artificial intelligence business value to reach $1.2 trillion in 2018

Global business value derived from artificial intelligence (AI) is projected to total $1.2 trillion in 2018, an increase of 70 per cent from 2017, according to Gartner. AI-derived business value is forecast to reach $3.9 trillion in 2022.

The Gartner AI-derived business value forecast assesses the total business value of AI across all the organisation vertical sectors covered by Gartner. There are three different sources of AI business value: customer experience, new revenue, and cost reduction.

“AI promises to be the most disruptive class of technologies during the next 10 years due to advances in computational power, volume, velocity and variety of data, as well as advances in deep neural networks (DNNs),” John-David Lovelock, research vice president at Gartner, said. “One of the biggest aggregate sources for AI-enhanced products and services acquired by organisations between 2017 and 2022 will be niche solutions that address one need very well. Business executives will drive investment in these products, sourced from thousands of narrowly focused, specialist suppliers with specific AI-enhanced applications.”

AI business value growth shows the typical S-shaped curve pattern associated with an emerging technology. In 2018, the growth rate is estimated to be 70 per cent, but it will slow down through 2022. After 2020, the curve will flatten, resulting in low growth through the next few years.

“In the early years of AI, customer experience (CX) is the primary source of derived business value, as organisations see value in using AI techniques to improve every customer interaction, with the goal of increasing customer growth and retention. CX is followed closely by cost reduction, as organisations look for ways to use AI to increase process efficiency to improve decision making and automate more tasks,” Lovelock added.

“However, in 2021, new revenue will become the dominant source, as companies uncover business value in using AI to increase sales of existing products and services, as well as to discover opportunities for new products and services. Thus, in the long run, the business value of AI will be about new revenue possibilities.”

Breaking out the global business value derived by AI type, decision support/augmentation (such as DNNs) will represent 36 per cent of the global AI-derived business value in 2018. By 2022, decision support/augmentation will have surpassed all other types of AI initiatives to account for 44 per cent of global AI-derived business value.

“DNNs allow organisations to perform data mining and pattern recognition across huge datasets not otherwise readily quantified or classified, creating tools that classify complex inputs that then feed traditional programming systems. This enables algorithms for decision support/augmentation to work directly with information that formerly required a human classifier,” Lovelock continued. “Such capabilities have a huge impact on the ability of organisations to automate decision and interaction processes. This new level of automation reduces costs and risks, and enables, for example, increased revenue through better microtargeting, segmentation, marketing and selling.”

Decision automation systems use AI to automate tasks or optimise business processes. They are particularly helpful in tasks such as translating voice to text and vice versa, processing handwritten forms or images, and classifying other rich data content not readily accessible to conventional systems. As unstructured data and ambiguity are the staple of the corporate world, decision automation will bring tremendous business value to organisations. For now, decision automation accounts for just two per cent of the global AI-derived business value in 2018, but it will grow to 16 per cent by 2022.

Smart products account for 18 per cent of global AI-derived business value in 2018 but will shrink to 14 per cent by 2022 as other DNN-based system types mature and overtake smart products in their contribution to business value. Smart products have AI embedded in them, usually in the form of cloud systems that can integrate data about the user’s preferences from multiple systems and interactions. They learn about their users and their preferences to hyper personalise the experience and drive engagement.
Existing IAM solutions are creating major barriers to digital technology adoption

Digital transformation is a much-hyped business buzzword, driven by the adoption of cloud IT services around the world. This hype has seen enterprises scramble to become more digitally agile in a fight to stay competitive. In fact, a new study by OneLogin reveals that 92 per cent of UK enterprises have developed a digital transformation strategy, with over two-thirds of those surveyed expecting to deploy up to 100 new commercial software as a service (SaaS) apps and on-premise apps in the next twelve months alone.

However, there is a fundamental flaw in their progress to a more digital future, navigating and securing the digital network across a combination of legacy IT, on-premise and cloud platforms. This is where Identity and Access Management (IAM) solutions have a role to play but are falling short of unifying all corners of the corporate network.

With more cloud applications coming into the corporate network and employees switching between on-premise and cloud applications daily, the corporate network has become more complex than ever before. It is therefore unsurprising that almost 90 per cent of the 250 IT decision makers surveyed see IAM as an important, if not critical, part of their digitalisation strategy.

Yet the survey results reveal a strong link between the barriers to digital transformation and the pain points they feel with their current IAM solution. Key barriers to digital transformation include a fear of spiralling costs (40 per cent), legacy systems (46 cent) and project complexity (37 per cent) and the major pain points for existing IAM solutions are cost (43 per cent), complexity (45 per cent) and fragmented access control for multiple environments (22 per cent).

Enterprises need IAM to progress their digital transformation strategies, but there is clear demand for a solution that supports every end-point of the complex corporate network, regardless of whether it’s cloud-based or on-premise.

Research reveals
Blockchain will be as transformative for business as the internet

New research from Intrinsic Insights has revealed that after reduced costs, the main benefits of Blockchain technology are greater data security and protection against cyberthreats.

Nearly nine in ten technology professionals believe Blockchain technology will be as transformative for business as the internet has been. At a time that concerns over data are at their highest, blockchain technology is considered a very adept way to provide greater privacy.

“In a world of increasing concerns over the security and integrity of our data, individuals and businesses are realising the inherent benefits that applications built on blockchain technology can provide when keeping people’s data private,” Dominic McCann, CEO of BTL Group, who commissioned the survey, said. “This research also illustrates just how many businesses are looking at using blockchain and of those that are yet to explore it, there is a significant proportion looking to do so in the next two years.”

After two years of high profile and successful Blockchain projects, learning how Blockchain can be developed better has test launched Interbit, its multiple blockchain platform, a next-generation platform that has unique ‘chain joining’ capability specifically created so that developers and businesses can quickly, easily and securely build applications.
Robots are a welcome addition to the workforce

With employers struggling to find people with the skills they need, even for entry-level jobs, industrial workers are increasingly seeing the benefits of working with robots, rather than humans, to improve productivity and relieve the pressures they are under. This is one of the findings of the latest research from Epicor Software Corporation, a global provider of industry-specific enterprise software to promote business growth.

According to the research, which questioned around 2,500 business respondents in 14 countries, staff are aware of the many benefits of working alongside robots. Over half (54 per cent) say robots automate repetitive or mundane work that they would otherwise have to do themselves, and 34 per cent agree that robots are more efficient than humans in the workplace.

It’s not just their efficiency that makes robots attractive co-workers; a quarter (27 per cent) cited the fact that robots do not get involved in office politics as a benefit of working with machines.

To find that humans are happy to work alongside robots is good news for employers that want to use cutting-edge technology, to plug a growing skills gap on their factory floors. The same research found that the industrial workforce is getting older and that only a quarter (23 per cent) of businesses are currently able to attract recruits with the right knowledge. The use of robots can introduce efficiencies where human resource is low, and they can also encourage young talent into industry—with 33 per cent of millennials wanting to work at the cutting edge of new developments.

Other research backs up the discovery that rather than being worried about job losses, workers are actually ready and willing to embrace robot co-workers. For example, the OECD has found that only about one-in-ten jobs are actually at high risk from automation, and Gallup’s latest study shows that only a quarter (23 per cent) of workers are worried about losing their jobs to AI.

Many employees are aware of the benefits of automation because they already have first-hand experience of robot workmates. A third (31 per cent) says AI, robots, and highly automated machinery are now a common feature of their day-to-day work, and only 32 per cent says they are not part of their workforce at all.

Those that work in finance, and those that work in the Asia-Pacific (APAC) region may be more up for working with robot co-workers than anyone else, 47 per cent of respondents in APAC agree robots are more efficient than humans (compared to 29 per cent in Europe and Middle East) and 33 per cent of those who work in finance agree robots can take stressful tasks away from humans (compared to 23 per cent in IT and 20 per cent of CEOs).

“The study shows us that the use of robots is a very real, but also very welcome way of solving an otherwise worrying industry-wide knowledge and skills gap,” Terri Hiskey, vice president, product marketing, at Epicor said. “With employers struggling to find candidates with the right skills or knowledge for entry-level roles, and with employees struggling to keep up with the pressures of business growth, automating aspects of the workforce offers a new way of building efficiencies into the supply chain, and enabling digital transformation. However, businesses need the right infrastructure at their heart if they are to manage data flows effectively and to make the most of robotics and AI. This is where ERP and the cloud come into their own.

“Far from workers worrying about their jobs being taken by robots, our study shows that employees are actually very happy to work alongside machines. With all the advantages of robots not getting involved in office politics too, we can expect to see more of this in the future.”
IoT, robotics and machine learning set to transform the supply chain

Transport and logistics businesses are investing in Internet of Things (IoT)-based smart technologies to help them take advantage of the wealth of opportunities that the fourth industrial revolution offers. This is according to research data collected by Inmarsat, the provider of global mobile satellite communications, which reveals that the sector is prioritising IoT, machine learning and robotics to increase efficiencies across the supply chain.

Inmarsat’s ‘The Future of IoT in Enterprise’ report, featuring responses from 100 large global transportation companies, found that respondents see IoT as the top priority in their approach to digital transformation, with 36 per cent having already deployed IoT-based solutions, and a further 45 per cent expecting to roll the technology out by 2019.

The research further revealed that transport companies are rapidly exploring a wide range of other next generation technologies in the pursuit of digital transformation. The most popular are machine learning (37 per cent), robotics (37 per cent) and 3D printing (29 per cent).

The supply chain looks set to be one of the biggest beneficiaries of this drive towards digital technologies, with 14 per cent already reporting visibility and efficiency improvements in their supply chains and a further 65 per cent expecting to achieve this in future.

Commenting on the findings, Mike Holdsworth, director of transport at Inmarsat Enterprise, said: “The industry is clearly making significant strides towards digital transformation, with IoT-based solutions, used in conjunction with robotics, automation and machine learning, helping to transform the way that goods are manufactured, stored and delivered. Companies that proactively invest in these technologies will be able to facilitate more secure and profitable operations across their supply chain.

“Connected machines that can quickly locate and retrieve stock, self-navigate through any environment and make automatic route corrections based on real-time information updates will prove invaluable for any logistics organisation,” he continued. “Smart robots and unmanned aerial drones that work without rest breaks, carry heavier loads and quickly bypass areas of heavy traffic or congestion will be hugely important. They will enhance supply chain management, while their ability of to self-diagnose faults and schedule predictive repairs will be vital for minimising downtime and reducing maintenance costs.”

EXPANDING
Rockwell Automation has expanded the FactoryTalk® Analytics portfolio, a robust advanced analytics environment that empowers users with the ability to quickly and confidently make informed decisions. These latest advancements were developed to reduce the complexity of the operations environment for manufacturers and producers and their employees who are driving operations.

VISIONARY
PTC has been positioned in the Visionaries quadrant by independent industry analyst firm Gartner in its first Magic Quadrant for Industrial IoT Platforms. PTC was placed highest for ability to execute and furthest to the right for completeness of vision overall.

INNOVATION
NI has released LabVIEW 2018. For decades, LabVIEW has led the industry in platform software for test workflows. Engineers can exceed their speed of innovation with LabVIEW 2018 by taking advantage of new tools that simplify system integration and grant more control through hardware accessibility.

COMBINATION
PA Consulting Group has acquired Sparkler, a leading digital insight and strategy consultancy. Sparkler’s customer insight, brand strategy and service design expertise complements PA’s existing innovation, digital and strategy expertise. The combination of PA’s and Sparkler’s capabilities will help clients to seize the opportunities of disruptive change.

PARTNER
Aspen Technology has joined the SAP PartnerEdge programme as a partner that designs, develops and builds software using the SAP HANA platform. Through its participation in the program, it is now announcing the availability of the Aspen Mtell prescriptive maintenance software, which runs on SAP HANA.
The UK has a rich manufacturing history. Despite our strong global ranking, the country’s manufacturing productivity has flatlined at less than one per cent since 2008 and a combination of challenges arising from Brexit in conjunction with global market volatility has seen growth slow down significantly since the start of 2018.

Fortunately, the convergence of connected technologies represents a new paradigm for industrial operations and the associated buzzwords, neologisms and acronyms that have dominated the media over the last few years have become firmly embedded in our industrial workplaces. Now it is not only CIOs and other senior management who are conversant in the latest developments in IoT, AI, automation and SaaS, but also shop-floor staff, machine operators, trainees and apprentices who are entering the factory environment for the first time.

The many benefits arising from digitally connected, autonomous production lines and supply chains connected to an intelligent cloud-based IIoT infrastructure will enable manufacturers – large and small – to operate with greater resilience, agility and flexibility. This ability to automatically harvest and analyse potentially huge volumes of data in real-time from multiple lines, plants and even from regions across the globe will offer unprecedented enterprise visibility and transformation. Eventually the maturation of these technologies will instigate the emergence of highly sophisticated value chains that will create new revenue streams through greater product customisation and personalisation as well as entirely new business models.

Before the digital revolution, factory datasets were inputted manually in paper forms or excel spreadsheets. Some organisations resistant to change still maintain this analogue approach to quality and process control which will inevitably have a negative impact on the scalability of their business, and this is further complicated by the question of whether manufacturers should prioritise investment in talent or technology? The next-generation workforce will expect to have the latest technology at their disposal, and failure to proactively invest in a digital transformation strategy will inevitably mean top talent flows towards manufacturers that do. Unfortunately, investing in industrial digital technologies while ignoring the need for a highly-skilled, well-trained workforce will mean that innovation will not happen, and the potential value of those investments will remain unexploited.

While we mostly read about Industry 4.0, smart factories or the factory of the future, depending on the choice of vernacular, we fail to recognise the importance of hiring new talent to enter the manufacturing workforce. The underlying catalyst for change could come from existing managerial teams with fresh agendas, new executives specifically brought onboard to drive this transformation or from external pressures in the form of economic, competitor, market or consumer trends. There will be some manufacturers who have not even considered digital transformation, while others may be fully immersed in building an IIoT network of smart factories, but the clear majority will fall somewhere between that spectrum. Before blindly jumping on the industry 4.0 bandwagon, each manufacturer needs to undertake a thorough analysis of their unique business and markets to identify the key strengths, weaknesses, threats and opportunities that will pinpoint where digital transformation will have the biggest impact. From here, key decision makers including CEOs and CIOs can begin devising a strategy for technology investment, trade partnerships and human capital that will be essential for building a robust operational infrastructure.

Having an appropriate programme in place for both technology and talent acquisition will ensure the digital transition is smooth, successful and cost effective. Once an approach is agreed, manufacturers can put initiatives in place that will create a confident, tech-savvy workforce, comfortable interacting with automated machines, data analytics and smart production lines.

The next generation of engineers, apprentices and students will gravitate towards organisations that display forward-thinking and innovation with a genuine appreciation of technology and its role in the future of manufacturing. This is intrinsically tied to talent acquisition and talent retention and there needs to be a fine balance across both talent and technology investment if UK manufacturers hope to survive and thrive within a highly competitive and protean international landscape.
ACCELERATING THE DEPLOYMENT OF IOT IN THE ENTERPRISE

Neil Bosworth, UK manager, Gemalto M2M looks at why industry has been slower than consumers to embrace a digital lifestyle

The last couple of years have been a turning point for the Internet of Things (IoT). In addition to the steady momentum of connected watches, light bulbs and security systems amongst technology enthusiasts, the explosive popularity of the Amazon Echo in the last few months has demonstrated that the IoT is now a mainstream reality.

Small scale experimentation and proof-of-concept IoT ideas has been commonplace, but to be truly worthwhile projects need to be able to mature and scale quickly. The technology and connectivity needed is here, but many organisations still need assistance in realising the opportunities they can bring.

The new world of connectivity brings almost limitless possibilities, and that can be a daunting prospect. Large scale projects that aim to connect tens of thousands of endpoints will undoubtedly be complex tasks which may well require a bespoke IoT connectivity and sensor solution. However, not every use-case is the same, and there are several industries and sectors where smaller scale IoT projects can thrive in the near-term – areas such as predictive maintenance, remote monitoring, building management, agriculture and fleet management.

Adding connectivity to the devices in these sectors can have a dramatic effect on productivity. In the cases of predictive maintenance and remote monitoring, sensors can be installed that monitor performance in real-time and send alerts and diagnostic information as soon as a fault is detected. This can prove to be a faster and more cost-effective way to resolve a malfunction when compared with using human employees, who may have limited technical skills with which to identify and resolve any problems.

Once the most appropriate areas for near-term IoT projects have been identified, there are several factors to consider that will help speed up deployment. Firstly, organisations should consider off-the-shelf IoT service terminals with pre-built generic functionality, rather than jump straight into bespoke development. This alone could take months or even years off a project’s timeline.

Secondly, they need to consider the organisation’s readiness for IoT and take steps to prepare. This means building a strong business case to parts of the organisation that may not be able to visualise the benefits of IoT investment. It also means assessing the internal skills base and working within its limits. In the case of maintenance, retraining service engineers may also be necessary, since supporting remote diagnostic flaws picked up by IoT solutions could be very different to previous diagnostics work.

From a purely technological standpoint, organisations also need to be aware of the wider IoT landscape, and how factors like connectivity standards can vary from country to country. They also need to make early decisions about the types of data collection and transmission that are required – from how frequently it is collected and how it’s shared, to the form factor of the data itself (be it raw data, text, sound, image or something else). Where the data is processed is also important – on the IoT device itself, in a cloud platform or when collected by the ultimate IoT management application.

Finally, security of data cannot be forgotten. If an endpoint is compromised, at the very least it could result in multiple service calls to an otherwise functioning machine, which could drive up costs and undermine trust - in both the specific system and the wider promise of the IoT.

A connected future

By adding connectivity to currently offline machines managed as part of a business operation – whether that’s vending machines, elevators or something else. And by taking the right steps, it can happen much more quickly than you might think. What’s clear is that barriers to entry are falling fast, meaning tasks such as maintenance can be revolutionised and made exponentially more efficient. But to achieve those benefits, organisations must focus on what’s achievable in the near-term, understand the nuances of the ways in which IoT projects evolve from prototype to production, and the ways in which they can accelerate that process. If more organisations can do that, perhaps 2018 will be the year IoT makes a real mark in the enterprise.
Service data is not just a missing piece of the jigsaw but a key piece that can add crucial intelligence around manufacturing performance and profitability. But service data intelligence is also outpacing the executive skillset. Here’s how you can harness it for your advantage.

“We need more data diversity,” Bernard Marr, analytics and big data expert, said when speaking in Berlin at a recent Big Data conference. “Companies that do well are usually more diverse and have more diverse data sets,” he added. The problem though, and Marr accepts this, certainly in recent LinkedIn posts on Big Data, AI and engineering, is that the technology development and data generation is moving too fast for us to keep up.

So, what are the five key things executives need to do, to become data experts for their organisation?

Beware of data hype

Everything for the past few years has been about Big Data and now Big Data and AI. The industry conferences are loaded with speakers telling businesses to “just do it”, just jump on that data wagon and roll. But what’s the point unless you align your data strategy with your business strategy? Executives should not fear Big Data but use it to help enhance business processes and decision making. What are the core goals of the business and how can using data to understand products and customers better help you achieve those goals? Surely if the data is not helping you make money and improving customer experiences or services, then it is not worth having.

Start small and focus

Data for data’s sake? Focus on an area where you know it could have the biggest impact. Field service data for example, would give a business evidential support on product performance through diagnostics, but also highlight any inefficiencies in how products are serviced. Are engineers being sent to the wrong jobs geographically? Are they turning up with the right tools and spare parts? Are the products they are repairing showing consistent problems; in which case the R&D department would be interested to know for future models. Are customers ready for an upgrade, and can sales teams be alerted? Focussing on an area such as service, a traditional sot centre will help businesses understand how data can be beneficial to multiple departments.

Play clever detective, not mad scientist

Executives need to direct their data scientists to discovering new business insights using the datasets and tools at their disposal. They need to be creative and use their experience, their gut instincts to determine where products are working well, where there are consistent faults and issues and where perhaps the business is losing money and can improve. The data will help support theories or offer alternative viewpoints. It can show inefficiencies but also provide evidence for improving processes and practices. Can cost centres become profit centres? How can the organisation monetise the data once it has been captured?

Know your data, lakes and gravity

Not all data is equal of course, so gaining an understanding of how data can be harvested, which datasets carry more weight and where it all ends up could have some benefit. Data lakes are repositories for raw, unstructured data, that is not defined until it is needed, which can be a problem for manufacturers. Data gravity is where data grows in weight and attracts applications and additional data towards it as it flows through an organisation. Service data, for example, is becoming richer and heavier because multiple pillars of master data are being linked together – customer data, product data and performance data.

Prepare for disruptive decision making

With technology we can connect everything to everything. Both the cost and benefit increase due to the integrated and holistic nature of Big Data. If the executive responsibility is only for one domain and the data spans multiple domains, then getting a decision on the business case involves a plethora of executives. That is disruptive to the legacy decision making model. It means restructuring decision making processes especially as demand for increased productivity and performance means more analysis of data will be done in real time.
The number and types of connected devices are increasing at an exponential rate. Gartner estimates that there will be up to 21 billion connected devices by 2020. With this growth comes increased opportunity, but also danger. When a market is growing at such a rapid rate, one thing becomes crucial: testing.

In a burgeoning market, customers are rightly sceptical of the potential for absolute connectivity. To convince them, customers need to be reassured of two things: that it is functional, and that it is safe. The most efficient and effective way of ensuring these is through testing.

**Functionality and user experience**

The Internet of Things (IoT) relies on a complex combination of factors including data, devices, services, sensors and networks and these all have different testing requirements. It is vital to rigorously test all different parts of an integrated system before it is launched, or any updates are made. When one of the key selling points of a connected device is to be always on, a single functionality issue could be your ruin.

Welcoming a connected device into your business should be a seamless process that makes a worthwhile difference to your life. This means that first impressions matter: if a user has trouble using their smart assistant for the first time, this could put them off all smart assistants for life. For connected devices to succeed, they need to have fast response times and an intuitive user experience.

**Security**

Another major barrier to the success of the IoT is customer fears about security. Connected devices are, by definition, part of a network of other IoT-enabled devices, leading to fears that if one is hacked, then the others will follow. When DDoS attacks increased 91 per cent in 2017 due to unsecure IoT systems, all security gaps needed to be thoroughly tested for and fixed immediately. Consumers will not buy into a product, or a sector, that they can't trust.

Ensuring faultless security can be challenging when new weaknesses are constantly being discovered. Companies need to integrate safety features into their design when developing devices and experienced security experts need to perform assessments on each application. Similarly, stringent testing is vital to safeguard products from any security gaps. Human and automated testing should play a key role in finding both superficial and substantial errors that can't be found in a lab context.

**In-the-wild testing**

As the number and type of connected devices proliferates, so does the number of things that could go wrong, whether that's a functional error or a security one. Further, they are being subjected to wildly unpredictable human environments. The traditional approach to testing, carried out by a small QA team working in the lab, is no longer adequate. It's impossible to recreate this environment inside a laboratory and there's a strong chance that they will miss out on some fatal errors.

The truth is that some errors can only be discovered by the user. Consequently, it is vital that devices are tested by real people on real equipment and in everyday situations, not in a laboratory, we call this ‘in-the-wild’ testing. In-the-wild testing enables software testers to react to constant changes and updates occurring in the IoT and reflect the real-life user experience much better than in a lab. Results gained from in-the-wild testing should, where possible, be translated to automated test cases, which are fast, iterable and cost-efficient.

The major barriers to the implementation of any new technology are firstly, functionality and secondly, security. If either or both are missing, it will be doomed to fail. Never has this been clearer in the IoT. If connected devices are to last, they will have to exist in a bug-free zone. And therefore testing is paramount.
Dealing with disruption

Rajat Dhawan, Bernd Heid, Paul Küderli, and Kevin Laczkowski of McKinsey look at how industrial companies can respond to disruptive forces

A survey of 300-plus executives from the automotive, aerospace, and diversified-industrial sectors generated insights that can help traditional players reckon with change.

The industrial sector will see more disruption within the next five years than it has in the past 20. Revenues will grow, but incumbents are ill equipped to capture their fair share. They will need to shake up their business models, their approaches to competitors, and the very core of their businesses to hold their own, let alone grow, in the face of a disruptive onslaught.

McKinsey sought to understand the implications of disruption in three industrial sectors: automotive, aerospace and defence, and diversified industrials (building and industrial technologies, machinery, and power equipment). We spoke to more than 300 senior executives from incumbents, start-ups, think tanks, governments, industry associations, distributors, and resellers around the world.

The head of a semiconductor company summed up the situation facing the semiconductor sector: “We’ve had technology disruptions before, but the market was stable. Now the market is being disrupted as well as the technology.” What can incumbents do?

Disruption does not have to be bad news: companies that can capitalise on it have incredible opportunities, and disruptive forces will raise revenues in all these industries. Most industrial sectors will, however, find it hard to adapt quickly enough, and not all of today’s leading players will retain their positions. As one business leader said: “We will see a complete reshuffling of the industry, and a shakeout will happen. The end game is not clear.”

Insights

Our survey produced three sets of insights that will be both provocative and helpful as companies consider how best to answer the disruption. The first relates to the disruptive forces themselves and to the ability of companies to prepare for them, the second to the implications for incumbents of the new disruptive world, and the third to the way companies can deliver a sustained, successful response. Ultimately, the findings suggest that piecemeal solutions will fall short of what’s required. Riding the disruptive wave is going to take courage, vision, and grit.

Incumbents are grappling with five disruptive forces

Executives identified five forces that incumbents must address simultaneously to have any hope of capturing the increase in industry revenues:

1. Connectivity-driven business models, such as pay per use and data monetisation
2. Artificial intelligence (AI) and autonomous systems, which go far beyond driverless vehicles and encompass machine learning and robotics
3. The Internet of Things (IoT), which could have an annual economic impact as high as $11.1 trillion by 2025, according to the McKinsey Global Institute (MGI)
4. Electrification, driven by regulatory and technological changes and by growing consumer demand
5. Cybersecurity, which is growing in importance as connectivity increases between and within companies, production facilities, defence systems, and so on
We asked respondents to rate the impact of each disruptive force on their businesses, from one (no effect) to five (affecting at least half of the business), and to rate their readiness, from one (no measures in place) to five (holistic transformation started). Worryingly, the gap between readiness and impact is substantial in several areas, including cybersecurity, connectivity-enabled business models, AI and autonomous systems, and the IoT.

Although incumbents and start-ups agreed on the impact of each disruption, the latter see themselves as much better prepared. This confidence should be a wake-up call for incumbents, although the start-ups still haven’t proved that they can scale up. As the CEO of an automotive start-up put it: “Classic players are weak and completely unprepared. My experience is that start-ups do not have to fear incumbents, because they are able to act much faster.”

**Disruption is upending the core of industrial companies**

To capture the growing revenue pool, incumbents must understand what the speed of change, the evolving competitive landscape, and the impact on the workforce mean for them. But the new world is very different from the one they know. The drone market, for example, is expected to leap from $6.4 billion today to $23 billion by 2024. However, the additional revenue will come largely from software and services rather than manufactured products, so incumbents are losing revenues to attackers.

The pace of change is startling. Three-quarters of the executives cited speed as a major challenge. Companies that are keeping up with it realise that speed is not just about making faster decisions; the scale of change and the potential impact mean that those decisions must be more radical.

The competitive landscape is also changing fast. Incumbents are under attack from start-ups on one side, and tech giants on the other. (At a recent automotive trade show, several journalists reported that the bosses of major German car manufacturers were more anxious to attract Facebook CEO Mark Zuckerberg to the event than they were about Tesla or competition from China.) But a third of executives still see other incumbents as a threat.

Finally, disruption will have an enormous impact on the workforce. Even with technologies already in use, MGI research shows that 45 per cent of the activities people are paid to perform today could be automated and that so could about a third of the constituent activities of 60 per cent of all occupations.

**What can incumbents do to stay relevant—or win?**

Faced with these challenges, incumbents need to reassess how they work or even what they are. Business models need to change; competitors may become partners; resources must be moved boldly, not timidly; talent acquisition must change; and agile must be transformed from a barely understood notion into the way critical parts of the business are run.

Different business models will be essential. Companies need to shift from a focus on clever technology and instead think about business models from the outset. Pay per use is one of the most prominent ones we see emerging.

Even air is being sold on a pay-per-use basis. Compressor provider Kaeser offers usage-based contracts: customers pay only for the compressed air they use. Kaeser installs and operates the system, guarantees performance, and splits the efficiency savings with the customer.

Smart thinking like this extends to recalibrating notions of competitors, customers, and partners. Manufacturers, suppliers, and service providers must form alliances or join ecosystems, even with companies they might have traditionally seen as rivals or never thought about at all, for investment, for skills, or to build platforms that integrate entire industries.

Airbus, for example, is partnering with Uber to
make it possible for people to book helicopters for a taxi service (an idea tested at the Sundance Film Festival); with hardware start-up investor HAX to develop, test, and commercialise vertical people-transport solutions for cities; and even with transportation-software company SITA to develop advanced cybersecurity solutions for the air-transport industry.

With so many avenues to explore, companies need to understand how to allocate resources appropriately. Basing budgets on last year’s spending is futile. So is moving a small share of money to a glamorous new digital idea. A third of our survey respondents believe that technology disruptions will make it necessary to reallocate more than 30 per cent of the resources of their companies.

The evidence backs up their opinion. Companies that actively reallocate resources perform significantly better than their peers. Companies that move more than half of their capital expenditures over a 20-year period generate almost two times more growth in total returns to shareholders than companies that move less than 30 per cent.

Some incumbents are adopting a zero-based approach to challenge their entire base spending, which can help shift mind-sets and money to where they are most needed. A European machinery player that shifted from a new-installation business to a service-based one built a hypothetical ‘model company’ simulating how its business might develop in different markets. This helped it determine where it had too much capacity, which products to abandon, and how to secure its profitability.

As we mentioned, automation will displace employees, but the disruptive forces also require fresh skills. Data scientists, AI experts, and programmers are all in high demand. In the United States, 100,000 software engineers will be needed until 2030 just to cope with the increased complexity of in-vehicle software. As one automotive supplier told us, “We have to change from a mechanical-gear-cutting company to a technical and analytical company. The challenge is scarcity of talent!”

Half of the companies we spoke with expect to acquire such skills through M&A or partnerships. Other companies are turning to crowdsourcing for the skills they need. GE, for example, reduced the weight of a jet-engine bracket by 80 per cent through an online design competition. The winning design was awarded $7,000, so the company, in effect, received thousands of person-hours of work at a fraction of the normal cost.

In response to the disruptive forces, respondents agreed most of all on the need for agility. Yet there is a huge mismatch between understanding the need for speed and taking measures to achieve it. Only a quarter of the respondents’ companies had initiated pilots or undertaken any sort of programme to become more agile. An agile organisation can implement new business models effectively, EBITDA margins, time to market, and frontline productivity all improve. The challenge is that there is no one formula for becoming agile; the starting point and context for each organisation are different. Nor must every part of the organisation be agile, though the whole operating model must change where agility would be of great benefit. However, almost three-quarters of companies implement only a couple of quick fixes, despite evidence that success is three times likelier when companies adopt much more comprehensive agile programmes.

A menu of topics for incumbents to address is helpful but not sufficient. Industrial companies that want to build and grow through disruption will need to undergo a complete change.

Most survey respondents have already begun company-wide programmes, some transformations are well under way. For example, a leading European industrial company decided to build an IoT–digital business, and that required a thorough transformation. In less than a year, the company successfully tied connected services into its core product offering. At each stage of the process, it focused on its customers’ needs and initial reactions to guide the transformation.

Transformations are daunting and can hit many obstacles. Companies are asking employees to be faster, more entrepreneurial, and less risk averse. Meanwhile, the way people work is changing all around them with the rise of digital technologies, automation, and cybersecurity concerns.

Three challenges stand out. First, companies will have to become more courageous. Daring to be ambitious and to make (and learn from) mistakes will help companies redefine themselves. Second, companies must ensure that the transformation is inclusive. It is essential to have a strong commitment from the top, cascaded down through the organisation and empowering all levels of employees to make improvements. Finally, companies must ensure that the transformation goes far beyond technology. In our extensive experience—backed up by our survey results—the biggest stumbling block for any transformation is usually corporate culture. As an automotive-OEM executive said: “The issue is not the organisational model; the issue is people and mind-sets.”

DEALING WITH DISRUPTION
Pointing the way to IIoT success through open standards and secure networks

Phil Beecher, president and CEO, Wi-SUN Alliance explains why standardisation is a key requirement for IoT projects

The Industrial Internet of Things (IIoT) is rapidly changing the way organisations work, for the better. Many across the globe are already driving improved collaboration and business efficiencies, faster time to market and productivity enhancements off the back of IIoT systems. Yet while the industry is maturing fast, there are roadblocks. Nearly 94 per cent of the global IT leaders the Wi-SUN Alliance polled recently who said they had IIoT plans, claimed they have experienced challenges, including security concerns, cost and an absence of leadership buy-in.

It’s clear from our detailed research into key IIoT verticals that security, performance and industry standards will be key to driving successful projects going forward.

Supporting the business

There’s no doubt that the Internet of Things is already responsible for huge investment in what can broadly be termed industrial projects: areas including utilities, smart cities, manufacturing, agriculture, transportation and even healthcare. The IIoT utilities sector alone is estimated to be worth $11.7bn by 2020, while the smart cities market is predicted to reach $147bn by 2020.

We focused our research on sectors that could specifically benefit from IIoT solutions including oil and gas, government, telecommunications, energy and utilities. Perhaps unsurprisingly, given their long-term use of SCADA and industrial control systems, oil and gas firms were most keen to adopt IIoT technologies. Utilities firms challenged with monitoring and controlling large, complex infrastructure systems, were also ready to embrace new technologies, with 78 per cent highlighting IoT as a top priority for 2018. But they weren’t alone in their enthusiasm. In total, over half of all the IT leaders we spoke to who are investing in IIoT claimed they have fully implemented their strategy, while around a third are currently rolling it out.

So why such an overwhelming response? We found that IIoT neatly ties into and supports many related business/IT priorities: 64 per cent cited increased IT automation, 55 per cent pointed to better use of big data analytics and 49 per cent highlighted improved connectivity as key focus areas for the year ahead. The most popular direct reason for embracing IIoT was “to improve network intelligence and connectivity for citizen safety and quality of life” (47 per cent), followed by improving system reliability (41 per cent) and reducing operating costs (37 per cent).
Real world benefits

The good news is that almost all IT decision makers said they’re already seeing some tangible internal and externally facing benefits after implementing IIoT projects. That’s why increasing numbers of big name organisations are putting their money behind such initiatives. It’s particularly popular among utilities players like Florida Power and Light, which runs a smart network comprising advanced metering infrastructure (AMI) and automated feeder switches (AFS) to serve over 4.5m homes. It’s not only reduced operating expenses, because many meter checks can now be carried out remotely, but also improved billing efficiency for customers: a clear win-win. It crucially also helped the utility avoid 118,000 customer outages during 2016’s Hurricane Matthew, with 99 per cent of those affected getting power restored within two days.

The benefits of a smart, connected grid are that you can also expand and enhance it with new capabilities. That’s what Florida Power and Light has done, adding nearly 500,000 connected street lights in what was the largest programme of its kind in the world when launched. This has allowed the provider to improve the reliability of its street light network; reduce usage and save money by dimming at certain times; and even provide emergency responders with the ability to control street lights on demand.

Oklahoma Gas & Electric has rolled out a similar smart grid, allowing it to lower emissions, give more control on energy usage to consumers and reduce costs by minimising the number of support vehicles on the roads. Its expandable network connected 250,000 LED street lights to improve quality of service and lower energy consumption. There are projects like these occurring all over the world, including major European cities such as London, Glasgow and Paris.

The security challenge

That said, there are challenges to running successful IIoT projects, with UK respondents to our study most likely to have encountered difficulties. In fact, only three per cent described the process as challenge-free. Security came out top (59 per cent) among our respondents’ challenges, and proven security with multi-layer protection and continuous monitoring was considered “absolutely crucial” for smart city solutions (50 per cent) and smart utilities (40 per cent).

It’s not surprising to see why, given rising threat levels. Critical infrastructure (CNI) providers have always been a major target for financially motivated cybercriminals and state-sponsored operatives, but warnings have increased significantly in frequency over
the past 18 months. The National Cyber Security Centre (NCSC) and US authorities recently issued a joint technical alert about malicious cyberactivity carried out by Kremlin hackers. It follows previous warning from NCSC boss Ciaran Martin that the Russian Government is actively attacking UK telecoms, media and energy firms.

The impact of such attacks may currently be unknown, but a cautionary tale exists in the form of Ukrainian power companies, which were attacked in 2015 and 2016, leading to power outages for hundreds of thousands. Although these attacks are thought to have been highly sophisticated, with at least one involving the reflashing of firmware on key systems, they don’t have to be. The WannaCry and NotPetya ransomware worm attacks of 2017 spread quickly to cause widespread outages and chaos across multiple sectors. Not only did WannaCry cause an estimated 19,000 cancelled NHS operations and appointments, but together they cost major organisations hundreds of millions in lost productivity and service outages. Global shipper Maersk ($300m), logistics giant FedEx ($300m) and Nurofen-maker Reckitt Benckiser (£100m) were among those reporting major losses.

New compliance requirements for EU organisations will only fuel the need to invest in security when implementing IIoT. The General Data Protection Regulation (GDPR) and Network and Information Systems (NIS) Directive will give regulators the power to levy fines of up to £20m or four per cent of global annual turnover for non-compliance. While the latter applies mainly to CNI providers, the former could affect any firm processing data on EU citizens. Worryingly, just 43 per cent of IT bosses we spoke to claimed they are including data protection compliance in their IoT strategy. That could be a costly mistake.

**Board on board**

The challenges of implementing IIoT extend far beyond security. Getting board-level buy-in was a common issue, with 32 per cent of respondents citing a reluctance among senior executives to commit to projects and a similar number citing funding challenges. Just under a third said their bosses didn’t understand the benefits of IIoT while 37 per cent claimed competing priorities were a barrier.

It’s clear that executives need to be briefed more effectively on the benefits of smart technologies. Among these, the most common cited by respondents were improved business efficiency (54 per cent), enhanced customer experience (49 per cent), better collaboration across the organisation (48 per cent), increased agility (47 per cent) and reduced costs (45 per cent). It’s up to IT leaders to pick out key business decision makers and convey the importance of IIoT in a language they understand. Research like this and case studies of real life successes will certainly help.

**The importance of standards**

One unusual finding from the research was the importance of network topology (58 per cent) in planning an IIoT initiative. In fact, it came top of the list of criteria for the IT leaders we spoke to. The majority said they favoured a blend of star- and mesh-based networks. However, mesh models offer a series of improvements over star networks which make them a better choice for CNI providers, including greater resilience to hacking and signal jamming. Mesh networks are also built to reduce single points of failure and black spots and usually transmit short distances, meaning they’re more power efficient and better performing.

That’s good news, considering that performance (53 per cent) also ranked high among respondents as a criterion for evaluating IIoT solutions. It’s clear that IT leaders rate factors such as latency, bandwidth and bi-directional communications as key to their decision-making process.

Open standards are another key feature to look for in any IIoT network technology, as they reduce the risk of vendor lock-in and ensure organisations are following industry best practices. More than half of those we spoke to claimed standardisation was a key requirement for IoT projects, 45 per cent said that smart city IoT solutions should be built using industry-wide open standards, and a similar number (43 per cent) said the same for utilities projects.

It’s heartening to see open standards given the importance they deserve. One such standard to look for is the IEEE 802.1AR spec for Device Identity, which supports improved authentication of a device. By embracing these and other industry-agreed standards, IT leaders stand the best chance of success with their IIoT projects: not only in optimising the performance of networks and devices but also ensuring interoperability across systems. Standards are the key to protecting legacy assets, preserving ROI, reducing TCO and charting a course for continued IIoT success as technology rapidly evolves.

The IIoT market is predicted to reach $934 billion by 2025. The key for IT and business leaders looking to differentiate with their initiatives will be knowing where to focus their spend.
At the recent Hannover Fair, CTS editor Mark Venables caught up with Bill Ruh, chief digital officer at GE and CEO of GE Digital to chat about GE’s vision for the digital future.

GE launched its Predix portfolio at the beginning of 2016. Last year was the second full year of operations and they announced $1.4 billion worth of orders on Predix with $550 million revenue and saw strong double-digit growth going forwards across their portfolio.

“We have learned a lot in that time. Some of the things were hard lessons and some came in the normal course of learning,” Ruh says. “One thing that strikes me is that seven years ago when we started people would ask me, ‘why are you doing this?’ I don’t think anyone thought of digital as necessary in the industrial world. Then a few years after that they asked, ‘what are you doing?’ Because by then I think they got a sense that digital was important, but they weren’t sure how to approach it. Was it an IT project or a business project? Then we moved into a phase where they said, ‘how are you doing it?’

“Many companies are exploring it now. Research shows that about ten per cent of the industrial firms globally are engaged at a leadership level and I think that number is about right from what we see. But just about everybody is starting to make a move and the laggards are only a very small proportion. The thing that I’ve noticed this year is that people want to know what the results are.”

The three challenges

When it comes to challenges, Ruh cites three major obstacles that must be overcome for a successful digital implementation. “It’s leadership, talent and culture; you could say that leadership and talent are the same, but I break it up differently,” he says. “One thing we have discovered is that if you don’t start with an outcome, what you want to achieve, you are going to find it ends in disappointment. We see a lot of people start with the technology, let me connect, gather the information, do some analytics and see what comes out, and as a result there is a strong disappointment.

“To be able to define an outcome you must have people who understand the technology. If you go to a supply chain leader or a plant leader and they don’t understand the digital technology, they can’t envision how it can help them. You could find yourself slowed down because the leadership has not made the connection between efficiency, productivity and more revenue with how they can use digital technology to achieve this.”

When it comes to talent, Ruh explains that GE build a lot into its platform but only a small amount was being used. “A lot of our customers do not have Silicon Valley quality developers, so we needed to deliver more pre-packaged capability.”

Culture is an important element as well; the philosophy of using these digital tools is often at odds with the ethos of many companies. There is fear for their jobs, a fear that their knowledge is not as valuable.

“Those three things play a strong role in slowing adoption. For us we find ourselves working with partners who help to bring that capability to a customer. To succeed, start with outcomes, make sure you have the right talent to be able to leverage it; people must be brought on a journey. The last thing is that we have a playbook. If I bring you APM, I know I can get you value quickly and that gets you the ability to learn. Once we figured that out as the lead sale it has opened opportunities for the broader portfolio.”
**Dirty data**

A lot of the value in the GE portfolio and platform is data ingestion. In a pristine PowerPoint world it is assumed that all the data is perfect and understood. It is not. Ruh believes there is a reason that most data warehouse projects fail, it is because you were forced to write down every single ‘what is this element?’ and ‘what does it mean?’. “In the industrial world temperature doesn’t mean just temperature, there is a lot more to it depending on where and how you are taking the reading,” Ruh adds. “You have to have some knowledge about the asset and the nature of the sensors to get the most out of it, in which case domain knowledge becomes important to get value from analytics.

“The second thing is that most of this data is dirty. Sensors aren’t pure; they don’t give you perfect data all the time without understanding the domain. What we see is people reading the data, pumping it into some machine learning algorithm and getting very bad results because they don’t realise the inconsistency in the data. They don’t know how to throw away the bad data. You also often find that you have scarcity, and that sparse data assumptions are almost the worst thing you can do.”

All these problems with data require domain knowledge. This means that GE, along with competitors such as Siemens, Rockwell Automation and ABB, are best placed to win this battle. They have the domain knowledge and industry experience to understand how it works.

**Avoiding commoditisation**

Although this domain knowledge is vital, the knowledge and tools that are available from Microsoft Azure, Google Cloud and AWS are vital to the development of digital solutions. They can supply commoditised IT infrastructure that allows the industry experts to concentrate on adding value. “Certainly, it’s a freeing,” Ruh says. “The problem is when we started this journey it wasn’t visible that it was the right thing to do.

“Four years ago when we started this inside the company, Microsoft Azure was in a different place; nothing like as strong as they are today. Back then AWS offered much less of a service; it was a lot more compute and storage whereas today they offer orders of magnitude, more software capability.”

In the early days Ruh and his team visited Facebook and they talked about how they had built their own data centres and they saw the world as being white labelled computer hardware. “It seemed at the time like that was a good idea because we saw that many of the Silicon Valley
companies were white labelling and creating their own data centres. Facebook even had an opensource effort to give away those designs. It seemed at the time as if that would be a winning strategy.”

Ruh concedes that it wasn’t a winning strategy. The rate and speed of investment required for such a strategy was extremely high. “We were about two years into it when we said we would have to change our strategy,” he adds. “It is absolutely freeing if you can figure out which services to offer. It is freeing, but it’s not zero work, because for example, we find that we are having to do more and more monitoring because the monitoring ability we see out of them is good, but we still see problems that occur. Do I wish monitoring was as good as it should be? Yes. Is it? It’s nowhere near where it should be.”

**Competing from big cloud**

The stands at Hannover were full of the traditional IT and cloud companies, such as AWS, Google Cloud and Microsoft Azure offering out of the box solutions for industry, which on the face of it would seem direct competition to the offerings of the industry stalwarts. When the conversation turned to artificial intelligence (AI), Ruh made it clear that despite what many might have us believe, AI by itself doesn’t do anything. It needs the domain knowledge to make it specific. “The problem is AI without data is not very useful and other companies don’t always have the data sets; industrial firms aren’t willing to give away their rights,” he says. “We found ourselves being very clear on those rights, and we also have a large set of our own
IN CONVERSATION WITH...

AI is important. I say that because AI can tell you a problem is going to occur, AI cannot by itself tell you what the problem is. It can say ‘here’s a pattern, I’ve seen this pattern, and this is what usually happens’ but what it can’t do is tell you what to do about it. Do I fix it now? Do I fix it a month from now or a year from now? Those are very different cost structures.

“The thing is you need physics-based modelling and simulation to be able to optimise it and decide which of those three options is the right direction. People talk as if AI and machine learning can do everything, but they can only tell you the past. What they cannot do is predict the future, that is what modelling and simulation does – they are going to move from being dull to the most exciting area in the next five years because they are a crystal ball.

“Done right you can apply some AI techniques, but modelling and simulation are going to be where the most interesting value is. Unless you have a deep understanding of the domain I don’t think you are going to have the best models in the world.”

**Future growth**

As Ruh alluded in the beginning, GE were doing more than they needed to. “At this point we are focussed on striking good partnerships that can move faster, because speed is everything,” he continues. “We are more open than ever now to strike a new partnership and use someone else’s capability.

“The second thing is our unique offering with Meridian and our APM suite that has given us a fantastic number of very specific algorithms for reliability management. That is a unique capability that you would not gain through a partner.”

Ruh also considers that edge computing is a unique offering. “The hardware itself is commoditised and we can get it from anywhere, but what I mean is that we are finding ourselves building a capability to pump analytics close to the machines, manage them at volume and scale at the edges and connect that into control system. That is domain specific, the ability to control that environment and have it work with edge computing in a holistic way is not going to be achieved by a general-purpose supplier.

Before we part Ruh voices two thoughts about the digital future. First that it is the software that drives the business model, enabling companies to do things that they couldn’t do before. “The second thing, and this is one that I think worries people, is that we’ve lived for 100 years in an environment where people told machines what to do. We are moving into an environment where machines tell people what to do. “It doesn’t mean that people go away, but it does mean that machines can think faster and give insight so that people can be more efficient. We are moving to a world where unless your people, the culture, the way they work, they want to use that knowledge, you may find that you don’t get the desired results and you don’t survive.”
The adoption of augmented reality (AR) is only just starting to take off. But the full range of possibilities offered by these technologies means they have the potential to bring about a sea change in both our private and working environments over the next few years and decades. AR will change how we learn, how we make decisions and how we interact with our physical environment. It will bridge the gap between the digital and physical worlds, between man and machine — and will become even more important when combined with smart, networked systems.

AR will close the gap between our limited mental and absorption capacity and the ever-increasing quantities of data and knowledge we face in this world of virtual, digital products. We also currently face the limitation that, while our world is three-dimensional, we use two-dimensional screens and paper print-outs when making decisions based on data from the virtual world.

What is AR?

Broadly speaking, AR is a new way of providing information, and the authors believe that it will have far-reaching effects on how data is structured, managed and made available via the internet. Currently, users need to transform data provided on a two-dimensional medium into three-dimensional reality. If you have ever tried to follow a manual when setting up or repairing a slightly more complicated device, you will be familiar with the mental process involved, and how easy it is to get it wrong.

These difficulties are linked to the five senses and...
the way in which we process information. An estimated 80 to 90 per cent of the information we absorb reaches us visually. The cognitive load grows with every task and takes up a chunk of our available mental capacity. As we find it easier to absorb and process information visually, reading a text and then processing the information involves a greater cognitive load than hearing the information and/or seeing it presented in a visual format. There is some truth in the saying ‘a picture is worth a thousand words’.

In AR applications, the solution is to project digital data on top of the physical world, for example as an image, a 3D model or an animation, merging the real world with the digital. This approach is revolutionary because it always takes the context of the environment into consideration, so the right information is always displayed at the right time and for the right object or physical environment. This then reduces the mental effort required to overcome the cognitive distance, the gap between how the information is presented and the context to which it relates. Take the simple example of getting directions from a smartphone GPS app, remembering them, and then acting on them at the appropriate moment. This presents a much greater cognitive load than if the information were projected directly onto the windscreen in the driver’s field of vision, as has been done for some time now in vehicles with integrated heads-up displays.

HOW DOES AR WORK?

Essentially, AR solutions consist of a mobile device with a built-in camera, such as a smartphone, tablet or smart glasses, running AR software. When the device is pointed at an object, the video stream is analysed by a machine vision algorithm to identify the object. The device then loads the AR data, a 3D experience, from the cloud or server and projects this directly over the object. What the user sees is therefore part real and part virtual reality. Every time the user moves, the size and spatial representation of the AR image adapts automatically, or new graphical/written information is shown in the field of vision while old information disappears.

IKEA offers product illustrations and apps allowing customers to visualise furniture or decorative items in their own home.
What can AR do?

The mantra that experience is what counts might have been written for augmented (and virtual) reality, as real-life experience of these technologies is essential. The two authors attempt to substantiate the fields of application and core functionality with examples that are as concrete as possible. They define ‘three plus one’ core functional areas where AR adds value: visualisation; instruction, training and coaching; and interacting with and controlling products – plus applications that combine AR with the complementary (but distinct) technology of virtual reality.

AR applications based on the principle of visualisation provide a sort of x-ray vision, revealing internal features that are usually hidden. Medical technology manufacturer AccuVein, for example, uses the heat signature of a patient’s veins to generate an image, which is then superimposed on their skin. When a blood sample is taken, this increases the likelihood of finding a vein threefold.

Bosch Rexroth visualises the internal workings of its CytroPac hydraulic power unit. The 3D image that appears when the user looks at a certain point on the outer body displays various configurations for the interaction between the sub-systems and the cooling options available for the internal pump.

In terms of instruction and training, AR will deliver considerable savings. As we have seen, following written work plans and assembly instructions is often difficult and time-consuming. An onsite AR application can provide real-time, step-by-step explanations of the work process, ideally using smart glasses so that the operator has both hands free. This turns conventional manuals into interactive 3D holograms. In a pilot project, Boeing reduced the time required to assemble an aircraft wing by 35 per cent by using AR technology, and the number of employees who completed the task correctly first time rose by 90 per cent.

Providing remote support will be a key application of AR. AR devices will forward the image seen by the engineer on site to an expert at headquarters, who can then talk the engineer through the operation or display instructions in the engineer’s field of vision. Lee Company, which sells and maintains

BOEING TESTS AUGMENTED REALITY IN THE FACTORY

Installing electrical wiring on an aircraft is a complex task that leaves zero room for error. That’s why Boeing is testing augmented reality as a possible solution to give technicians real-time, hands-free, interactive 3D wiring diagrams - right before their eyes.

“A person working in an industrial setting has a lot of distractions in that environment and a lot of data to think about and process,” Brian Laughlin, IT tech fellow, says. “Traditionally technicians had to look at and interpret a two-dimensional twenty-foot-long drawing and construct that image in their mind and attempt to wire based on this mental model. By using augmented reality technology, technicians can easily see where the electrical wiring goes in the aircraft fuselage. They can roam around the airplane and see the wiring renderings in full depth within their surroundings and access instructions hands-free.”

Paul Davies, Boeing research and technology associate technical fellow, is working closely with the programme and Boeing IT to develop and test augmented reality technology on the tanker. “Our theory studies have shown a 90 per cent improvement in first-time quality when compared to using two-dimensional information on the airplane, along with a 30 per cent reduction in time spent doing a job.”

Bruce Dickinson, vice president and general manager of the 767/747 Programme added that the cross-functional team working on this technology has made a step-change break-through in quality and productivity by following their passion to pursue a great idea. “We don’t often see 40 per cent improvements in productivity, and I’m convinced that it was a culture of innovation and leaders who are willing to say ‘yes’ that enabled this idea to come to life,” he adds.

A Boeing technician in Mesa, Arizona uses a wearable augmented reality device to look at instructions while assembling an electrical wiring harness. Using augmented reality can help improve first time quality in the manufacturing environment.
building systems, saves $500 in labour and travel expenses per technician each month and calculates a return of $20 on every dollar invested in AR.

While we currently control and interact with products or machines using buttons, handles or, more recently, even integrated touchscreens, AR will bring this to a new level. For example, factory staff wearing smart glasses can use gestures and voice commands to control virtual control panels and can check and adjust machine parameters while walking through the workshop without physically touching the machines themselves. Although this functionality promises huge potential, it is still in its infancy; especially when it comes to commercial products, and working environments are in dangerous or remote areas, or where the scenarios involve future or past situations. As the fourth core function of AR, VR provides the virtual background reality for the three other core functions. Audi is currently testing the VR holodeck, an accessible, virtual environment where the 3D image of a car can be used to evaluate designs during the transition from development to production. The US Department of Homeland Security is combining AR instructions with VR simulations to train disaster relief workers in responding to dangerous situations, like explosions. In a similar vein, the energy company BP uses VR to simulate drilling conditions as a backdrop for AR training procedures. Both companies are using these technologies to reduce costs and risks.

Two ways that AR can add economic value

In principle, AR can be used in two different areas of application. Firstly, it can add value to a product and secondly, it can help to further streamline processes in all areas of the company, from product
Ford designers have been swapping some clay-sculpting steels and rakes for mixed reality headsets and visualisation software that can change vehicle design elements – side mirrors, grilles, vehicle interiors and more – in mere seconds. Designers have been piloting Microsoft HoloLens technology for a year now in Ford’s Dearborn studios, allowing them to see proposed virtual design elements as if these pieces were part of physical vehicles. They’ve been able to explore different shapes, sizes and textures of future vehicle attributes in minutes and hours instead of the weeks and months it can take to create clay models. And now, Ford is expanding this pioneering testing across the globe.

“It’s amazing we can combine the old and the new, clay models and holograms, in a way that both saves time and allows designers to experiment and iterate quickly to dream up even more stylish, clever vehicles,” Jim Holland, Ford vice president, vehicle component and systems engineering, says. “Microsoft HoloLens is a powerful tool for designers as we continue to reimagine vehicles and mobility experiences in fast-changing times.” HoloLens technology uses mixed reality, which enables designers to see holograms in photo-quality backdrops through wire-free headsets. They can scroll and preview at the flick of a finger through numerous design variations projected virtually onto an actual car or clay model.

“We may not be able to teleport yet, but HoloLens allows us to review full-size 3D designs with designers and engineers around the world in real time,” Craig Wetzel, Ford manager, design technical operations, says. “And we’ve only just scratched the surface, so possibilities for the future seem almost limitless. This is very exciting.” As designers wearing headsets move around an actual vehicle, the HoloLens scans and maps the environment far more accurately than GPS to render holograms and images from the angle at which the vehicle is being viewed. A Windows 10 computer embedded in the headsets brings the power of the operating system to a holographic device that is untethered, wearable and mobile. Traditionally, designers and engineers must wear headsets that rely on cables tethered to a PC. Designers see 3D holographic images of themes and features as though these elements were already part of the vehicle, allowing them to quickly evaluate the design, make changes, and determine styling options earlier in development.

Ford has adapted HoloLens technology to enable designers to collaborate with engineers to better understand the customer experience, too. For example, the technology allows a designer and engineer to evaluate in near-real time how a new side mirror looks aesthetically, as well as the customer’s view of the vehicle’s surroundings. Whereas today it can take days, even weeks, to study a grille design, HoloLens allows designers and engineers to explore a
development and manufacturing to sales and service. In products, for example, using AR to display instructions or safety information can represent a unique selling point. Heads-up displays have been available in cars for some time now and have also been used in aeroplanes for several years. If these displays are too expensive, an app for smartphones or smart glasses can be provided; this can be used to create a personalised virtual display to set up and operate the product.

Although 3D design models have been used in product development for many years, they are still represented using two-dimensional technology, hindering the creation of an integrated design process. With AR technology, full-size 3D models can be projected as holograms in the physical environment. For example, the 3D hologram of a construction machine can be ‘installed’ in its future working environment, and developers can walk around and climb into the full-size model to test lines of sight or ergonomics. And, while Volkswagen previously used 2D drawings to laboriously check the quality of prototypes, the company now uses an AR application to merge the prototype with the 3D model, making the process ten times faster.

In manufacturing, operators are given exactly the right information at the right time for the numerous manufacturing steps at their workstations. They are also given monitoring or diagnostic data for the systems, allowing them to perform proactive maintenance. In manufacturing and assembly environments, AR is also very effective for training purposes. In logistics, removing items from shelves using a paper list makes up 65 per cent of warehouse costs. At DHL, AR applications have improved the order picking process by 25 per cent by guiding workers along the shortest path through the warehouse. These kinds of solutions can also highlight the relevant storage bin and specific storage location in colour.

AR also offers a wide range of possible applications in marketing and sales. Showrooms and product demonstrations will offer fascinating, personalised customer experiences, and products can be viewed in their actual target environments, which will also support online retail. IKEA offers product illustrations and apps allowing customers to visualise furniture or decorative items in their own home. Aftersales service can also benefit greatly from the step-by-step repair assistance and remote support made possible by AR technology. In some circumstances, customers may even be able to get involved in maintenance work and perform many of the tasks themselves. This will deliver considerable savings when it comes to service.

variety of different iterations in a matter of hours. The headsets can even be synced to allow multiple team members to view a design simultaneously, making collaboration easy. Beyond the global design test, Ford is investigating how to bring HoloLens technology into more engineering development processes to further bolster the company’s lead in using advanced visualisation technologies such as virtual reality. “HoloLens allows a whole team of people to collaborate, share and experience ideas together,” Elizabeth Baron, Ford virtual reality and advanced visualisation technical specialist, says. “Mixing virtual and physical models is exciting, because it helps our designers and engineers communicate effectively and ideate to see what the future looks like earlier in the process. This allows great freedom and efficiency in how prototypes are created or changed.”
Deploying AR

As we have seen, the full range of technical possibilities offered by AR is already being exploited for many applications. Although most of these are still at the pilot testing or PoC (proof of concept) stage, each AR installation requires a carefully thought-out implementation plan. This clearly identifies the strategic benefits of the application and sets out the technical and organisational solutions and skills required in detail. Porter and Heppelmann pose several questions relating to the deployment of AR.

The first question is: “Where does AR knowledge come from?” Specialists in AR development are scarce. The required skill set includes user experience or user interface design (UX/UI design), handling of 3D data and models and their implementation in AR applications, and, most importantly, content creation. Products (static 3D models) in different environments (such as IKEA) are relatively easy to create. Dynamic 3D content, such as instructions or training in manufacturing applications, presents a greater challenge. The most complex apps involve interactive solutions using technologies that have not yet reached maturity, such as gesture or speech recognition.

Regardless of the application, how the content is created has top priority. To obtain detailed digital images of products, CAD models can be adapted from product development or technologies such as 3D scanners need to be used. Advanced AR applications must also connect to business systems or other external data sources such as sensors so real-time data can be incorporated into the content. Last but not least, the decision must be made on whether a standalone software app should be developed or whether a content publishing model with content from the cloud would be more appropriate.

Most AR applications currently run as apps on mobile devices such as smartphones or tablets. Although the use of wearables such as head-mounted displays (HMDs) and smart glasses is still only just starting to take off, these devices are rapidly gaining ground in production environments. The idea is that, instead of carrying screens in their pockets, users will wear smart glasses as second nature, like sunglasses. In any case, the race is on to produce the best smart glasses, given that the company that dominates this market will also have a degree of control over AR technology. However, initial experience with the technology indicates that there will not be one set of universal glasses for all applications. For example, a Microsoft HoloLens in its present form will not be suited to harsh production environments. Devices like the smart glasses from the German manufacturer Trivisio would perform better here and can also be tailored to individual customers’ needs.

To summarise, Porter and Heppelmann believe that AR is an innovation of historic significance, and it is hard to disagree with this assessment.

Bosch Rexroth visualises the internal workings of its CytroPac hydraulic power unit.
Bright sunlight floods the Volkswagen Virtual Engineering Lab in Wolfsburg. Two dozen screens flicker, some of them showing graphics and others hundreds of lines of program code. In the centre of the room, there is a scale 1:4 model of a Golf. Frank Ostermann inspects the model, and then he changes its wheels, replaces the rear lights and modifies the wing mirrors. Ostermann uses voice commands and gestures to change the design. It is all completed in a matter of seconds. Augmented reality makes it possible. The software required was developed in the Virtual Engineering Lab and the team’s results could revolutionise the work of engineers and designers.

Ostermann is wearing HoloLens mixed-reality goggles. The mobile computer developed by Microsoft projects virtual content onto a physical object through gesture control and voice commands. Ostermann only needs to point his finger and the HoloLens projects a different paint colour onto the Golf, installs different wheels and modifies the fenders. Initially, the Golf is an R-Line model, but it then becomes an entirely new version. Perhaps this model will appear at the dealership in six months’ time.

Ostermann is a graduate engineer in computer engineering. At Volkswagen in Wolfsburg, he heads the Virtual Engineering Lab, one of six labs now operated by Volkswagen Group IT in Wolfsburg, Berlin, Munich and San Francisco. The latest lab is currently starting operations in Barcelona. At these labs, specialists from Volkswagen are working on the digital future together with research institutions and technology partnerships. New solutions in the fields of Big Data, Industry 4.0, the Internet of things, connectivity, mobility services and virtual reality are being created in close co-operation.

“At Volkswagen, we have been using augmented reality and virtual reality for some time, mainly to obtain a three-dimensional view,” Ostermann, says. “We are now taking a major step forward at the Virtual Engineering Lab. We are transforming this technology into a tool for technical development. This will allow Volkswagen engineers to work on a virtual vehicle, to change its equipment as they wish and even to design new components virtually. They will be able to see the results of their work immediately.

“We are co-operating very closely with our colleagues from Technical Development and are already close to the first new vehicle concepts and design studies. We contribute our know-how for technical product development and offer tailor-made solutions for all group brands in the fields of virtual engineering and systems engineering.”

What is the reason for this approach? Augmented and virtual reality help save time and development costs. Each step in the process can be made faster and more efficient, for example with HoloLens software from the Virtual Engineering Lab.

The HoloLens not only projects each design or equipment change directly onto the physical model. It also allows several project teams to work at the same time but at different places, for example teams from Wolfsburg, Chattanooga and Shanghai. All concerned always have the current design model in view and time-consuming reworking, for example on a clay model, may become a thing of the past. “The teams can directly follow and compare minimal changes to the model and then make a decision. This means that they can reach their goal faster,” Ostermann explains.

Currently, the HoloLens software is still in the trial phase. In future, it will allow users to call up the entire Volkswagen brand model portfolio and to present different body versions of a model in all conceivable variants: the developers will then be able to transform a saloon virtually into an SUV, an estate car, a convertible or a coupe.

“Just a few years ago, this was all science fiction,” Ostermann, says. “Now it is clear that this is how we will be developing our next models.”
The latest trends in cybercrime have seen it all. Advanced exploits allegedly developed by high-profile threat actors used in massive ransomware attacks, creativity of spam and phishing attacks on trending topics, and attacks relying heavily on social engineering or legitimate software used as cyberweapons. This evolution of cyberthreats calls for evolution in cybersecurity.

“The ever-changing threat landscape means every business faces unique risks and challenges, even with the most advanced anti-malware protection in place,” Russ Madley, UK head of channel at Kaspersky Lab, says. “As threats continue to grow in complexity, it’s important cybersecurity companies continue to ensure their customers are protected with the most up to date security software.”

The scale of the cybercrime threat to manufacturing cannot and should not be underestimated. In a recent survey of UK manufacturers carried out by EEF, nearly half said they have been the victim of cyber-crime, and a quarter have suffered some financial loss or disruption to business as a result.

The manufacturing sector is the third most targeted for attack, with only government systems

As digitisation accelerates, it’s critical for organisations to shore up their defences to ensure information systems are well protected, as Mark Venables explains.

GERMAN STEEL MILL MELTDOWN

While the exact details of the company involved are still unknown, the attacker used sophisticated social engineering and spear-phishing tactics to hack into the steel mill’s office computer network. Crucial controls were tampered with, making it impossible to turn off the blast furnace. The result - massive damage to the foundry.

The attacker, likely an industry insider or someone working with an insider, had specific knowledge of the production processes involved so that maximum damage could be done to the normal workings of the mill. The company’s systems were specifically vulnerable because the office network was connected to the industrial control system, meaning the attackers could effectively take control of production – and stop it from happening.
and finance more vulnerable. Yet manufacturing - which has 2.6 million employees, provides 10 per cent of UK output and 70 per cent of business research and development - is amongst the least protected sector against cybercrime in Britain.

The report pinpointed the susceptibility of manufacturers to cyber risk, revealing that 41 per cent of companies do not believe they have access to enough information to even assess their true cyber-risk. And 45 per cent do not feel that they do not have access to the right tools for the job.

Cyber threat is holding back companies from investing in digital technologies, with a third of those surveyed nervous of digital improvement. Moreover, a worryingly large 12 per cent of manufacturers admit they have no technical or managerial processes in place to even to start assessing the real risk.

One of the easiest forms of cyberattack comes through poorly protected office systems, often the first implemented historically within manufacturing businesses. The report looks at a number of real-life examples, including two where companies production systems were infiltrated and severely disrupted after hackers gained access to their IT systems by initially hacking into unprotected office software, used to keep HR and admin records.

“More and more companies are at risk of attack and manufacturers urgently need to take steps to protect themselves against this burgeoning threat,” Stephen Phipson, CEO of EEF, says. “EEF has a vital role supporting manufacturers in the face of this challenge and we are working closely with RUSI, whose world-leading Cyber Security Research Programme is well established as a key voice to understand the fight against the threat of ever evolving cybercrime to the modern business.

“Failing to get this right could cost the UK economy billions of pounds, put thousands of jobs at risk and delay the supply of essential equipment to key public services and major national infrastructure projects. I hope this report underlines the critical risk to government and industry”.

Romaney O’Malley, head of UK regions and head of industrials at insurance company AIG Europe explains that for many manufacturers, cyber-risk is still not considered a principal risk on the risk register. Nevertheless, the cyberthreat landscape has evolved over the last year, with attacks becoming more sophisticated and more broadly disruptive.

“There is an increasing level of state-sponsored attacks between nation states, where companies infected by malware may just be collateral damage. The potential threat from cybercrime is widespread,” he says. “There is evidentially significant need for greater awareness and understanding of the importance of cyber-risk management, not only to protect existing businesses, but to create more secure environments to grow and capitalise on the potential that digital technology advances bring to manufacturers.”
Searching for the weak spot

According to ‘Paradigm Shifts’, Trend Micro’s security predictions for 2018, skills and resources are the two elements that make up an attacker’s arsenal. An attacker, however, cannot set out to break security or even perform sophisticated attacks without finding weak points in a system first. Massive malware attacks, email-borne heists, hacked devices, and disrupted services all require a vulnerability in the network, whether in the form of technology or people, to be pulled off.

It goes on to say that increased connectivity and interaction over insecure networks are a given. Unfortunately, poor implementation of technologies adds to the likelihood of threats being realised. Having protection where and when it’s needed will become the backbone of security in this ever-shifting threat landscape.

“In 2018, digital extortion will be at the core of most cybercriminals’ business model and will propel them into other schemes that will get their hands on potentially hefty payouts,” the report adds. “Vulnerabilities in IoT devices will expand the attack surface as devices get further woven into the fabric of smart environments everywhere. Business email compromise scams will ensnare more organisations to fork over their money. The age of fake news and cyberpropaganda will persist with old-style cybercriminal techniques. Machine learning and blockchain applications will pose both promises and pitfalls. Companies will face the challenge of keeping up with the directives of the General Data Protection Regulation (GDPR) in time for its enforcement. Not only will enterprises be riddled with vulnerabilities, but loopholes in internal processes will also be abused for production sabotage.”

These are the threats that Trend Micro feels will make inroads in the 2018 landscape. As such, they will serve as further proof that the days of threats being addressed with traditional security solutions are behind us. As environments become increasingly interconnected and complex, threats are redefining how companies should look at security.

Balancing risk with IOT benefits

The British media widely reported how the recent WannaCry cyberattack largely targeted NHS trusts across the country. However, what was not as widely reported was that the attack also affected many factories across the world, shutting down production and causing concerns about data security.

“No plant manager can deny that the internet of things (IoT) has had a substantial impact on the plant that they run,” Steve Hughes, managing director of power quality specialist REO UK, says. “They now have the ability to monitor, measure and optimise almost every process in their plant, using interconnected devices and control software such as SCADA.

“As British industries look to reverse the productivity crisis by optimising output in their factory, even small improvements in efficiency and quality can give a competitive edge.”

Although the interoperability of devices presents many benefits to the plant manager, it does present risks in terms of cybersecurity. Attackers that successfully penetrate a system can hold important and potentially sensitive data to ransom and can use the
interconnectivity of devices to shut down the entire plant."

Before plant managers introduce smart monitoring systems they should consult independent experts to perform a risk assessment and evaluate existing security measures. Plant managers should adhere to standards such as IEC 62243, which makes provisions for the network and system security for industrial-process measurement and control. This will limit the damage caused to employees, businesses and the wider industry from a potential cyberattack.

"Cyberattacks usually target conventional IT rather than operational technology (OT)," Hughes continues. "Because many monitoring systems such as SCADA are PC based, when the attack spreads throughout the network, this will affect the entire connected network of devices. Using PLCs will reduce the likelihood of this type of issue as they are not PC based. However, OT is not completely immune to the threat of cyberattacks, although these tend to be a form of industrial espionage rather than an external attack such as ransomware.

"We all know that IoT devices are good for our plants but the recent wave of cyberattacks is causing many to question their presence. However, with the right security measures in place, smart monitoring devices can play a pivotal role in the modern factory and should be embraced, rather than shunned."

INDUSTRIAL CONTROL SYSTEM ATTACK IN SAUDI ARABIA

In August 2017, a petrochemical manufacturer in Saudi Arabia was infected with malware that investigators believe was not simply designed to steal data or shut down operations but potentially to cause a catastrophic explosion. Significantly, it targeted operational technology in the form of industrial control systems rather than the more traditional focus on information technology. Whilst the identity of the company affected, and the likely attackers remain unclear, it has been revealed that the target was part of the facility’s safety system, designed to stop automated equipment going beyond safe operating conditions. The malware was designed to override this.

The attack was not intercepted by the cybersecurity measures in place and failed only because as the developers of the malware had made an error in the code that caused the systems to simply shut down safely. It is likely that the perpetrators will have since fixed this error.
Earlier this year Honeywell launched its first industrial cybersecurity centre of excellence (COE) at its Middle East headquarters in Dubai. At the opening CTS met up with Jeff Zindel, vice president and general manager, Honeywell Industrial cybersecurity for critical infrastructure & IIoT, to discuss the industrial cybersecurity landscape.

**Connected Technology Solutions (CTS): Does the increased threat of cyberattacks negate the value of connected technology?**

**Jeff Zindel (JZ):** The benefits of digital transformation and the power of connected technology are tremendous as we know in enhancing productivity, unleashing new value for companies, but critical is enabling it securely. Cybersecurity should be considered upfront in all digital transformation or IoT initiatives. The good news is that with Honeywell being a leading expert in the area we’re here to assist companies where they don’t have those specialities in-house.

**CTS: Does size matter when it comes to cybersecurity?**

**JZ:** I believe cybersecurity should be embedded and layered on top for all customers. Whether it be in high or low risk assets it really comes down to their tolerance of risk and the consequence of an incident or cyberattack and what that might result in. Based on the varying levels of cybersecurity controls and maturity we recommend depending on their risk profile and risk position. For us it is not so much about the size of the company or the size of the facility but the risk, whether it is a process disruption risk or a risk to the brand.

**CTS: Is a layered approach to cybersecurity still valid?**

**JZ:** We totally believe in layered cybersecurity because you have got to have different levels of protection and different levels of defences to protect you across an enterprise. But a defence in depth strategy is core to our view of cybersecurity and it is just a matter of the maturity of the site or customer.

**CTS: Are people still the weakest link in cybersecurity?**

**JZ:** People are and will be involved in most cases, so we advocate taking a
A holistic approach to cybersecurity addressing people, process and technology. It is critical to have the right policies, training and awareness in place, but again that is not enough. We advocate putting the right technologies in place, the right architecture to mitigate or minimise the impact a malicious or accidental action by an employee, vendor or visitor can have. We believe again to put in layered controls and technologies to minimise the risk of a cyberincident by a person or should unfortunately an incident occur, then to minimise the impact and layer in recovery actions, continuous monitoring in a way that provides insight. If you can’t block the action at least have the visibility into the action to be able to react quickly. I refer to them as insider threats, bad people meaning to do harm, and then there are insider risks, which is more often the case when you have an unsuspecting employee, contractor, vendor or visitor who is introducing malware or risk without knowing what they are doing. For the most part they are people trying to do a good job, but if you don’t have the right cybersecurity technologies and controls in place you are opening yourself up to tremendous risk.

JZ: It is part of our connected strategy across the corporation in connected plant. We are embedding cybersecurity technology in concert with our machine learning and analytics platforms to capture data in real-time and to gain insights.

CTS: How important will machine learning be to cybersecurity?

JZ: This is all based on proprietary, patented Honeywell industrial and OT cybersecurity understanding. What we are doing on a real-time basis is capturing information from devices and network flows to identify vulnerabilities, threat, and through algorithms translate those into indicators of risk. We are then scoring those risks and tying that risk back to concepts and industrial environment zones. We are looking at it from a perspective of zones and devices or areas or processes of greatest risk. We are scoring that and presenting that in a simple manner that a control engineer and all the way up to a cybersecurity expert of CIO could benefit from.

CTS: How should industrial companies measure their risk?

JZ: The threat is real. We are operating in industries and countries around the world and we are certainly seeing an increase in the number of attacks and the number of incidents in industrial environments. The good news is that we have solutions and there are technologies being introduced to help industrial customers. With digital transformation comes an increased focus by corporate leaders to move forward and protect assets and increase awareness to move forwards in a smarter way than they have in the past.

CTS: How can you marry the different security approaches between IT and OT?

JZ: With digital transformation comes an ever-increasing drive towards IT and OT convergence. That is the marrying of information technology with operations technology. We are increasingly seeing the digitisation of what were previously analogue instruments. To us the cybersecurity principles still hold and there is still separation. If you segment networks correctly, you separate them and put the right monitoring in place, put the right cybersecurity controls in place and you can certainly move forwards in a safe and secure manner. It requires in-depth understanding of industrial environments to safely and securely deploy cybersecurity technologies. As you know they are different worlds. You have plants that are running on five, 10 or 20-year-old technology in some cases. IT networks are different, they are not so concerned about the downtime so that is something that differentiates. We live, eat and breathe OT environments and enable that effective convergence with corporate networks.

CTS: How does the move to autonomous operations affect cybersecurity?

JZ: It is essential to have continuous monitoring in place, to have visibility into what is happening, to understand and baseline what I would call normal operations and be able to identify those process upsets or those anomalous activities or behaviours that would flag a concern or a risk. For us it is about continuous monitoring, we have developed a platform called The Industrial Cybersecurity Risk Manager that provides real-time visibility into vulnerabilities and threats, we also offer managed security services to our customers to provide 24/7 secure and remote monitoring and expert support to complement their staff or unmanned operations.

CTS: Is there a different approach between greenfield and brownfield facilities when it comes to cybersecurity?

JZ: Legacy equipment creates its own unique challenges because productivity, safety and reliability is the name of the game. You must be very smart about what technologies you deploy, what architecture changes we make and when we make them, how we operate within their operating
Environment when they have shutdowns and when we can make changes. Certainly, there are solutions for continuous monitoring, to proactively identify vulnerabilities and threats and build those layers of cybersecurity technology on top of that brownfield site. It is challenging but that is what we have been doing for 15 years. Over that time, we have learnt a lot and developed our own methodologies, solutions and own software to address some of these challenges.

CTS: Are we winning the cybersecurity battle?
JZ: I would never want to address the question as a battle. What we are doing is helping our customers significantly enhance their cybersecurity resilience and defences and drastically reduce the chance of accidental attacks. There are incredibly sophisticated state-sponsored attacks and it’s an ongoing challenge and an ever-changing environment.

Nation state attacks can be very well funded and are very sophisticated. It’s a challenge though that we look at when we work with customers to step back and take steps to not only increase their protection but to their resilience and recovery. If an incident can occur, what are the policies and procedures as well as recovery mechanisms in place to recover from that? We assume the worst with customers that have a risk profile that warrants it and then we plan back from that. An example is we work with customers on actual attack scenarios to identify what happens, who does what, what policy is in place, who has decision-making authority. Another simple example is testing the backups, not just making the backups but making sure you can restore the system. It's an ever-increasing, challenging environment that we operate in but that's not going to change.

CTS: What is the level of awareness when it comes to industrial cybersecurity?
JZ: I think there is a tremendous awareness and understanding by customers on a broad scale now of the need for cybersecurity in industrial environments. At the same time there is a tremendous shortage of industrial cybersecurity talent; there is a great shortage of skilled resources who understand the intricacies of operating technology in industrial environment. If they know cybersecurity they might just be an IT networking professional; they don’t know anything about the OT side. On the OT side you may have several process engineers, many of whom have grey hair today and they don’t understand IT network technology and cybersecurity. What we strive to do is to partner with customers, be they the most developed enterprise or a small individual plant, to help complement their teams of their lack of skill.

CTS: What does the future hold for cybersecurity?
JZ: In the future it is going to be leveraging the power of connection for cybersecurity to provide that visibility and real-time insight of what’s happening and to leverage the experts that can’t be everywhere at once. It’s also, though, to be looking at cybersecurity increasingly at a system of systems level rather than at a product, device or component level. While those are important at the core you have to have security embedded in each of your devices, more important is the interaction of those across a network or system. With the proliferation of connected devices, the need for cybersecurity across and over the top is more important.
It is a classic case of poacher turned gamekeeper. In his previous guise Jonathan Bennun was a hacker, now he is fighting against cyberattack as product strategy manager at access management provider OneLogin.

When he was attempting to breach systems, he found vulnerabilities like easy-to-guess passwords made his work much easier. “If that attack vector didn’t pan out, I could usually get around the authentication flow, or gain basic privileges and escalate them for admin access. We must accept that these vulnerabilities – imperfect authentication and passwords - are not going away anytime soon, and businesses must take steps to strengthen their security posture.”

A key challenge in eliminating passwords is that too many software as a service (SaaS) providers still don’t offer token-based sign-in such as with security assertion mark-up language (SAML) or authentication layers such as OpenID Connect. On top of that, many enterprises still have dozens - if not hundreds - of legacy applications that require passwords. “It will take some enterprises a long while to migrate off these legacy apps which use application-specific passwords, and do not support requirements such as password complexity or password expiration,” Bennun adds. “In addition, passwords make for only a small part of a strong security posture. Security is only as strong as its weakest link, and on some systems, passwords may be a good attack vector. Real-world attackers are more likely to use alternate attack vectors to get around passwords. Three of the most common are application vulnerabilities, spear-phishing and social engineering.”

Bennun explains that being a true password champion means applying password best practices while having a modern approach to access management that is more holistic than a password management tool or a password education campaign.

To explain what businesses are doing wrong and how they can fix it, Bennun uses the classic security triangle: people, process, and technology. “When it comes to people, enterprises invest in education like training for compliance reasons, but often overlook enabling people with self-service for password reset and self-registration of multi-factor authentication (MFA),” he explains. “In addition, companies combat shadow IT, but don’t offer an alternative such as faster onboarding of business apps. For example, your employees need to use LinkedIn and Twitter for business, so provide them with a safe way to manage passwords for those personal apps.”

When it comes to process, it is important to think marathon, not sprint. “Some SaaS providers still don’t offer token-based sign-in such as SAML-enabled login,” he says “Enterprises need to gradually consolidate passwords, ideally to a single set of corporate credentials for apps, networks, and devices. Similarly, access management should be unified and holistic across the entire organisation with user information and privileges.”

The final piece of the puzzle is technology. Password best practices are not hard to follow and apply, and they are an important part of any security practice. “Having said that, don’t stop there, and don’t look for a silver bullet,” Bennun concludes. “Look for a platform, not a tool, for the wide variety of use cases and for supporting complete authentication and access management scenarios across the enterprise. For example, a single platform can make it much easier to provide password reset self-service to your entire user base.”

In summary, being a true password champion goes well beyond password best practices. Enterprises that fail to deploy today’s front-line access management solutions across their organisation - enabling people, planning for a continuous effort, and seeking a full platform solution - are at serious risk and will lose out.
Large-scale adoption and immersion in cloud computing has increased significantly over the past few years – from email platforms through to HR and CRM services – as the benefits and understanding of what the cloud offers has been proven.

Security has been a key consideration at each stage of the cloud adoption cycle, as IT provision has moved from on-premise to outside a company’s walls. Equally, faced with simultaneously using private and public cloud along with on-premise providers, companies need to understand what entity is responsible for protecting which data asset.

To truly understand the cloud security journey and where we are now (and what’s next), we need to take ourselves back to a time when servers, software and most business operations sat in a building, and ownership and maintenance was someone’s responsibility.
Stage one: ‘Check out the size of my server’

With a server room on-site, the ability to ‘see and touch’ IT provision gave businesses peace of mind that their IT was safe. “They had complete control and ultimate responsibility, making security straightforward and something that could often be achieved with basic cybersecurity software and robust policies,” David Emm, principal security researcher, Kaspersky Lab, says. “But as demand on networks and bandwidth grew, and storage capacity reached breaking point, physical space to accommodate a company’s IT needs and the associated costs fast became a barrier to IT ownership. Cloud was the next natural step to lighten the load, but was often implemented to the detriment of security.”

Stage two: Growing up and out

Instead of holding everything in, the growth in cloud technologies allowed companies to easily expand their IT provision and keep up with the demands placed on their infrastructure by customers and the business. “But despite the promises, the advent of cloud was greeted with mixed emotion,” Emm adds. “The IT team became the driving force behind cloud as a way to meet efficiency and performance KPIs. But for IT security, a new element of risk was starting to creep in. Driven by business leaders wanting to achieve better performance and flexibility, cloud was fast becoming the way forward – but the security surrounding it was often an afterthought, with no strategic or joined-up approach. Spam, ransomware and data theft are just as big a problem in the cloud as they are on premise – and out of sight shouldn’t mean out of mind.”

Stage three: IT fights back

With the IT department feeling empowered, concerns were raised over the security of cloud services and the viability and visibility of off-premise solutions. “However, the IT security team often lost the debate, with the board and business directors dictating the case for cloud adoption. Security was often overlooked in favour of business gain,” Emm continues. “But, for all of the benefits that cloud adoption gave a company, it was also fast becoming a cybercriminal playground, and a haven for lucrative information and personal details. For many companies, in moving infrastructure to the cloud, they assumed that their provider would take responsibility for its security. So security was pushed down the priority list.

“However, this is not always the best strategy, as users of Amazon Web Services would testify. Misconfigured S3 cloud storage buckets left sensitive data unsecured and exposed, affecting numerous companies including Accenture, the US military, and the Australian Broadcasting Corporation (ABC), who have all experienced data leaks as a result. No matter what level of cloud services were being used, it quickly became clear that companies needed to take all means possible to secure their own data.”

Stage four: The C-suite pulls rank

Despite concerns, the C-suite’s desire for efficiencies are now seeing companies increasingly rely on cloud. Indeed, Kaspersky Lab’s own research has found that when it comes to software as a service, 78 per cent of SMBs and enterprises are already making use of at least one form of cloud service with three quarters planning to move more applications to the cloud in the future. Infrastructure is no different. With a quarter of companies already taking a hybrid approach and 24 per cent planning to do so in the next 12 months, the issue surrounding the security of a sprawling IT infrastructure should not be to the detriment of the benefits it offers.

Stage five: A new approach

With cloud computing now an accepted norm, its continued adoption is undeniable and unstoppable. “But security needs a different approach,” Emm concludes. “One that can secure even the most complex infrastructure and any cloud configuration. The nature of hybrid cloud adoption means that there isn’t a one-size-fits-all security fix, as there perhaps once was with on-premise provision. “Any solution needs to be flexible, manageable and performance-led, so as not to undermine the benefits of cloud. No matter whether you take a hybrid, hosted or private cloud approach, having visibility of what services and data reside where is the first fundamental step in protecting your business. Once determined, each part of the cloud infrastructure must have its own set of security measures and technology to protect your business from cyber-threats, just as you would protect any data and devices within the company walls.”

Cyberthreats will continue to evolve and target data, no matter where it is stored. Only by deploying security technology that uses a mix of machine learning and up-to-date threat intelligence can an organisation ensure the best protection for its chosen network environment and data.
The critical path to manufacturing efficiency

CTS looks at how innovative technology is enabling manufacturers to transform their processes with real-time insight into any aspects of operation

The connected technologies that underpin Industry 4.0 promise to transform manufacturing with real-time insight into any aspects of operation that risk degrading finely-tuned processes. But there is a problem – the way organisations can respond to that insight. Where is the prioritisation to guarantee that it is the most critical alerts that are attended to and minimise any business or employee impact? The information about the type of fault or the ability to track response? The dated paging and mobile systems in use by many companies are simply not enabling companies to achieve the promised improvements in operational efficiency.

Real-time information is of no value if it is not used effectively. “It is therefore essential to consider the critical path; to assess how the information provided by devices and sensors to deliver vital alerts could and should be used to facilitate the quickest response possible,” Klaus Allion, managing director, ANT Telecom, says. “It is the analysis of this path, the understanding of the steps needed to be taken, and the ability to design the most successful workflows that leverage smart communications solutions that will improve both processes and employee safety.”

Investment drive

The latest budget was full of incentives for manufacturing companies to increase their investment in capital stock in a bid to address the UK’s lack of productivity, under investment in equipment over the past decade and extended reliance on cheap labour. And to be fair, the opportunities for investment are immense given the current level of innovation and change. From Artificial Intelligence (AI) to robotics, the Internet of Things (IoT) to Industry 4.0, few manufacturing companies could be in any doubt that there are many ways to leverage innovation to drive productivity improvements.

But organisations cannot afford to look at innovative technologies in isolation. “IoT, for example, is all about providing real-time alerts from sensors or devices to inform operations, from highlighting temperature variations that could affect product quality, to revealing a drop in valve performance or raising the alarm of a lone worker accident,” Allion adds. “Fantastic, what company wouldn’t want an early warning of potential problems that could affect a finely-honed manufacturing process or employee safety?”

“But what happens next? How does the company respond to these alerts? Information is brilliant, but it is only of true business value if actioned intelligently to achieve measurable improvements within operations. The availability of real-time alerts in the event not only of machine failure, but machine degradation that could affect product quality is just the start. It is the way the company responds to the alert that makes the real difference. What is the process for ensuring the right people are informed and able to rapidly remedy the issue? How are alerts prioritised? Right now, this is where far too many manufacturing processes fall down.”

Critical path

Of course, manufacturing plants have been collecting alert information from machines for years, long before IoT exploded the devices and sensors available. Supervisory control and data acquisition (SCADA) systems for
remote monitoring and control are a standard component of any operating environment, providing a single view of equipment performance on a large screen in a control room. More recently, these systems have gone mobile, offering operators and maintenance engineers the chance to view the red, amber, green alerts on a tablet while on, or away from, the factory floor.

"That’s great, but the way in which organisations respond to these alerts is still, in the main, archaic," Allion continues. “A red alert could prompt a generic page message to which any number of individuals may or may not respond. Alternatively, an operator viewing the red alert on the SCADA screen must call the engineering team leader who will access a control panel to understand the true nature of the problem and only then identify and contact a team member to resolve the issue.

“Reliance on such dated communication models is clearly inadequate - especially given the cost, maturity and robustness of alternatives. An intelligent smartphone-based communication system can enable a far more interactive response - if companies reconsider the critical path.”

**Step by step**

Direct integration between a communication system and a control panel, for example, provides immediate information about the nature of the fault. Smart workflow then ensures the system automatically contacts the most relevant team, such as electrical engineering, eliminating several time consuming manual steps. Once the designated team member has received the smartphone-based notification, they can confirm their attendance and, critically, provide updates on the repair resolution.

This approach can be extended to that mass of often overwhelming SCADA data, replacing ad hoc decision making with automated, workflow-based processes that effectively prioritise and communicate requirements to engineering teams. “Rather than give the engineers the same mass of overwhelming red, amber, green information on a small tablet, just show the critical alert,” Allion says. “There are huge risks that a red dot will be missed amid a mass of other coloured dots – if it is a priority, make it clear: a massive red dot that stands out from the rest will ensure the engineer recognises the priority and responds.

“Reliance on such dated communication models is clearly inadequate - especially given the cost, maturity and robustness of alternatives. An intelligent smartphone-based communication system can enable a far more interactive response - if companies reconsider the critical path.”

**World of the future**

There is no doubt that over the next decade investments in robotics, AI and IoT will transform manufacturing processes. But whatever innovation is introduced to the production line, and the deep insight, sophistication and early warning these systems will give into potential issues, it will only deliver value if companies can respond intelligently and effectively.

In the Industry 4.0 world of the future, AI enabled machines may well be self-learning and able to auto-correct. In the meantime, it is those companies able to use a smart approach to communication, based on a fine-tuned critical path, that will be able to achieve the incremental efficiency gains demanded by a government keen to see the UK rise up the productivity ranks.”
3D printing, sometimes known as additive manufacturing (AM), is one of the biggest technological innovations of the decade. It is technology that can allow you to build anything from the ground up, so long as you have the appropriate schematic.

Additive manufacturing is set to revolutionise the way we do things. Imagine producing and manufacturing spare parts for equipment in remote locations like on oil rigs and in space? Or even purchasing, downloading and printing a tool for use immediately? The possibilities are endless.

Missed opportunities
More than half of the UK’s workforce lack awareness about the revolutionary benefits of 3D printing, which could hold back the economy in comparison to other, more innovative nations. In a survey conducted
by 3D printing specialist King of Servers, 88 per cent of respondents do not have a 3D printer in their workplace, while only six per cent said their workplace had invested in one to date.

Furthermore, 63 per cent went on to state that, to the best of their knowledge, their employer was not planning on purchasing a 3D printer. Simon Thomas, 3D printing specialist at King of Servers says it is concerning that the majority of businesses do not realise what the benefits are of the technology.

“I see every day how 3D printing can transform what is possible for UK businesses in a whole host of private and public sectors, so it is disappointing to know that the vast majority of people across the country are not given the chance to work with this revolutionary technology,” he adds.

Some 57 per cent of respondents said they were either unaware, very unaware or did not know about the benefits of 3D printing in the workplace. In addition, 45 per cent said they did not know to what extent their company could be improved with a 3D printer.

However, the data showed that among the few that did work with a 3D printer, 58 per cent would recommend the technology to another company or peer within their sector.

“The data, as well as anecdotal evidence when working with companies, shows that once a business invests in 3D printing, they find it hard to imagine going without the cost savings, return on investment and creativity that comes with it,” Thomas says. “I believe this lack of adoption could really begin to harm UK companies, setting the UK economy back further than economic rivals like the US.”

According to Sculpteo’s most recent State of 3D Printing report, Americans have more experience than Europeans when it comes to 3D printing (3.13 years compared to 2.82 years), while 3D printing is more integrated in American companies’ strategies (43 per cent versus 34 per cent). In addition, the report stated American firms tend to spend more money on external 3D printing services than their European counterparts.

Barriers to adopting 3D printing

In a briefing paper by Imperial College London, it was suggested that some of the main reasons for the slow uptake for 3D printers include the perceived high cost of 3D printers and materials, design tools that do not adequately exploit the full potential of AM and a lack of suitably trained professionals working with 3D printers. These challenges remain despite public funding for additive manufacturing research in the UK increasing from £8 million to around £55 million in 2016.

“It is disappointing to know that the vast majority of people across the country are not given the chance to work with this revolutionary technology”

Thomas

“Experts in the UK have been saying for years how 3D printers will revolutionise the businesses that embrace the technology, but in that time there has been more talk than action,” Thomas adds. “While it’s great to see that more money is being invested into research, 3D printing is still seen as something of a taboo in practical terms. ‘It’s a novelty product’ and ‘it’s just a phase’ are things I still hear today and, suffice to say, they are the exact same noises I heard when standard printing came about.

“One of the main barriers to adoption of this technology is perceived cost. However, many people are now surprised to find that 3D printing technology is considerably less expensive than they thought. In addition, the total cost savings and return on investment can be huge. One typical user case is where a global car manufacturer saved on average £600,000 per month with the deployment of low-cost, high quality 3D printers over multiple sites.”

How 3D printing works

3D printing works by turning a whole object into tiny slices, producing an item from the bottom up, piece by piece. These tiny slices glue together to form a solid object. Depending on the type of 3D printer, the heated extruder head moves in three dimensions while the printer lays down the filament, layer by layer. Each layer can be complex, meaning 3D printers can integrate moving parts, such as wheels and hinges, onto the same piece.
The materials used in additive manufacturing are instrumental in determining the look, feel and quality of the item printed,” Peter Morgan, product specialist from Elementar, explains. “The majority of 3D printers use Polyactic acid (PLA) or Acrylonitrile Butadiene Styrene (ABS) filament. However, metals, wood and even biological matter can be used to produce an object.

“The model of a 3D object is loaded onto a computer in a three-axis grid. The X-axis represents the side-to-side movement of the print-extruder head, the Y-axis represents the front-to-back motion and the Z-axis represents the object’s height.

“The printer software calculates the height of the component and analyses how the extruder and the build platform must move to lay down the filament layers. This process, referred to as slicing, sees the printed object’s height sliced into individual layers for printing. The software then converts the slicing data into a language known as G-code, which is effectively the set of instructions needed by the printer to carry out the task.”

Plastics in 3D printing

The most common type of plastic 3D printing is a process called fused filament fabrication (FFF). A continuous filament of a thermoplastic material is fed through a moving printer extruder head. Molten plastic is then forced out of the print head nozzle to create the item to be printed.

FFF can offer numerous advantages to businesses using 3D printers. “This is because the properties of plastics are extraordinarily diverse, with density playing an instrumental role in the malleability of the material,” Morgan adds. “Polyethylene (PE), for instance, is the most common plastic on earth, and can be manufactured at different densities to serve different purposes. For example, Ultra High Molecular Weight PE (UHMWPE) is used in bulletproof vests and Low-Density PE (LDPE) is used for disposable packaging like shopping bags.”

With the considerations above, plastic, as a material, is extremely flexible in terms of its application and as such, is amongst the best material to use for 3D printing.

When considering using plastic for additive manufacturing applications, it is imperative to ensure that the plastic used is of the highest standard. This is because a lower quality plastic will result in an inferior 3D print. Organisations supplying plastic for use in 3D printers should consider the quality of the raw materials used when providing their customers with the materials for FFF.

Elemental analysis holds the key to determining the quality of plastics on an industrial scale. “Spot checks using elemental analysers, such as inductar cubes, can help to determine the quality of plastic,” Morgan, continues. “Plastic contains additives to change the properties of the polymer, and, as such, may increase nitrogen and sulphur quantities within the hydrocarbon. These elements may give undesirable physical characteristics, resulting in a lower quality print. A simple elemental analysis will identify impurities in the plastic, safeguarding against low quality plastics being distributed.”

Metals in 3D printing

Materials used in metal additive manufacturing are predominantly metal alloy powders that are combined with heat from a laser to fuse them into a solid form. Other additives may also be used, helping to catalyse the formation of the process and alter properties of the finished product.

Powders must be used because it is not possible to accurately ‘spray’ a molten metal. They also...
offer a range of benefits over current methods of manufacturing metals, such as forging or casting from a metal stock. These techniques limit the potential shapes and structures that can be produced due to the physical restrictions imposed by the moulds used.

"3D printing largely removes these constraints as the structure is built up in layers," Morgan says. "This enables both the range and the complexity of the items that can be produced to be vastly increased."

**Checking the quality of a finished product**

The quality of the powders used in additive manufacturing is incredibly important because these powders will impact on the physical properties of the finished product. For instance, powder plays a crucial role in shaping the product’s tensile strength/brittleness, impact resistance, heat tolerance and resistance to corrosion.

As the process requires the combination of multiple powders, a precise understanding of the chemical composition of the finished product is required. The carbon, sulphur, oxygen, nitrogen and hydrogen composition will impact on the physical properties of the final product. This is because elements that were present at the beginning of the process, may be lost or altered under the heating process.

“For this reason, it is important to be able to analyse the final product to compare the product’s elemental composition,” Morgan explains. “By comparing ‘good’ and ‘bad’ products, it is possible to understand what differences there are in elemental composition between the two.

“Another important point to consider is that the powders used in additive manufacturing can oxidise over time. That being the case, it is vital to gain a firm understanding of how quickly this will likely occur and to discover more about how this oxidation will affect the finished item.”

How the future of additive manufacturing stacks up remains to be seen. However, the benefits of using powders - especially the removal of physical limitation of products - should mean them playing a hugely important role as the industry evolves and develops. Similarly, improvements in the quality of the powders used will help to increase the number of products that can be made.

“The current barriers to successful additive manufacturing are the physical properties of the alloys formed,” Morgan concludes. “They are brittle, and as such, cannot take the stress of a cast/forged metal item. When the technique is refined, it will be possible to produce 3D printed items cheaply. Right now, this is expensive due to the cost of the moulds that need to be created for the production of the piece. This is common with other items, such as plastics.”

With powders being vital to help revolutionise many industries, the importance of using high quality powders is clear. Additive manufacturing could play a crucial role in production in the years ahead - as such, it is imperative that the materials used are properly tested and analysed. With the right equipment, any fears that a powder is unsafe or unsuitable can be allayed.
Within the international glass industry, Zippe is renowned as the contact of choice for batch and cullet plants. Owner-operated in its fourth generation, the company was formed in 1920 and supplies everything from one source, from planning to commissioning. Forty-five experienced individuals are responsible for the realisation of modern, high-performance automation and control systems.

“Within our industry, successfully completed reference projects are frequently the deciding factor for being awarded an order, or not. It is therefore imperative that we deliver systems with a high level of availability, which are efficient and easy to operate,” Joachim Ullrich department head, Zippe, who places great value in selecting suitable hardware and software solutions, explains.

Glass production plants usually remain in operation for ten to 12 years, without interruption. Even if the plant only has to run for 16 of 24 hours, longer shutdown periods are still not an option. “A maximum of three hours, then production has to continue,” Ullrich confirms. He adds that reliably functioning

**BOTTLE JOB**

High-availability process control solution as a cross-discipline core of a newly erected smart factory where glass bottles are manufactured for the pharmaceutical industry

Within the international glass industry, Zippe is renowned as the contact of choice for batch and cullet plants. Owner-operated in its fourth generation, the company was formed in 1920 and supplies everything from one source, from planning to commissioning. Forty-five experienced individuals are responsible for the realisation of modern, high-performance automation and control systems.

“Within our industry, successfully completed reference projects are frequently the deciding factor for being awarded an order, or not. It is therefore imperative that we deliver systems with a high level of availability, which are efficient and easy to operate,” Joachim Ullrich department head, Zippe, who places great value in selecting suitable hardware and software solutions, explains.

Glass production plants usually remain in operation for ten to 12 years, without interruption. Even if the plant only has to run for 16 of 24 hours, longer shutdown periods are still not an option. “A maximum of three hours, then production has to continue,” Ullrich confirms. He adds that reliably functioning
systems are one of the main requirements of the glass industry. Especially as the Zippe plants are directly connected with the centre of the entire production system, the glass melting furnace.

“We take care of everything that has to happen prior to this step: From the delivery of the raw materials to their dosage and weighing, in some cases requiring precision to the exact gram,” Ullrich says. Across the almost 100-year corporate history, a total of approximately 600 batch plants as well as more than 1,000 cullet plants have been designed and implemented by Zippe in accordance with customer requirements.

Zippe is globally renowned for a wide range of skills. The ability to modernise existing plants during continuous operation is one of the major strengths of the Wertheim-based company. Plant designs, which provide precisely what the final customer envisages, are another specialty of the house.

GREENFIELD PLANT

During a greenfield project in France, Zippe was contracted to deliver a batch plant with mechanical conveyor technology and a cullet return system. With regards to the execution of this project, the following requirements had to be met: The plant should be designed to supply two furnaces with a total of 130 tonnes of mixture in 16 hours. Output reserves were requested, and the facility should allow three different types of feeding – big-bag filling, filling with silo trucks and mechanical loading. The plant had to be erected within one year and put into operation with the supreme satisfaction of the final customer. Finally, the utilisation of a PlantPAx ready system as a higher-level process control system was demanded - PlantPAx is Rockwell Automation's distributed control system. This should ensure a uniform look and feel at all operating and monitoring stations of the entire factory.

“We have already been working with Rockwell Automation in a highly successful manner for many years,” Ullrich says. “We were already supplying plants with Allen Bradley control systems as early as back in the 90s. The demand is increasing, especially in Australia, America and South Africa.”

The PlantPAx ready system is virtually predestined for sensitive applications, in which reliable around-the-clock operation is a requirement. This is because this process control solution not only guarantees a high level of availability via the redundancy of system components, but also by means of a device level ring topology in the EtherNet/IP network.

“The major advantage of the PlantPAx ready system is that it acts across different disciplines and combines the different areas – i.e. the continuous furnace control and the batch plant - into a joint network,” Ullrich continues. “Devices that actually communicate over a different protocol, such as, for example, the electronic systems for weighing or the barcode reader, can also be easily integrated into the higher-level process control system.” Ullrich is satisfied with an engineering-friendly solution that enabled Zippe to make an entire batch plant with mechanical equipment, with conveyor belts, with feed units, with motors, with screw feeders, with a large work with virtual production data, enter different recipes, produce thousands of batches and simulate an entire monthly production in order to avoid any ambiguities or errors in advance,” Ullrich
4,000 litre mixer, and the entire automation technology including control cabinets fully operational in only one year.

Ullrich adds that shortly after they were awarded the order, Rockwell was there and actively supported them in the selection of the appropriate components and in the design of the plant network. “The final customer is very satisfied with what we have realised together,” he adds, especially since enough reserves were planned and included on the system. The first small expansion, to integrate an additional raw material weighing system into the process control system has already been implemented.

The pre-furnace silo, that is the silo upstream of the glass melting furnace, demands replenishment in a fully automated manner if a certain threshold value has been on the batch plant. The supplies of sand, soda, dolomite and limestone are generally among the most important ingredients found in the production of glass and must be 100 per cent according to the recipe.

**VARIED MIXES**

The Zippe batch plants, however, need to potentially weigh other ingredients, in some cases with to-the-gram precision. “Every single one of our customers has his own special and secret recipe when it comes to the mixing ratio of the raw materials contained in his glass,” Ullrich explains. “The important thing is that the individual components are weighed precisely and within a certain period. This enables a new batch to be produced every five minutes.”

Consequently, in addition to the ‘calling signal’ of the pre-furnace silo, the weight signal of the weighing vessel is one of the most important pieces of information processed by the process control system.

Ullrich explains that this higher-level intelligence ensures that the silos are loaded correctly. “With the help of technical aids, we can ensure that sand does not end up in the soda silo,” he says. “By scanning the barcodes on the delivered raw materials, the control system sets the correct path. A wrong selection is then no longer possible.”

The system also proves itself to be very user-friendly when it comes to monitoring adjustable frequency drives. Drives are displayed on the visualisation stations with icons and faceplates and managed on the asset management level. In addition, disaster recovery functionality enables the system to automatically backup and restore the drive configuration as well as logging of changes. Extensive diagnostic information is delivered directly to the user on the HMI level.

The RA Process Library contains ready-to-use control and diagnostic objects. This allows the entire production process to be easily monitored: “Thanks to a seamless EtherNet/IP network structure, the technicians can route through right up to the variable frequency drives to retrieve individual variables or current signal states,” Ullrich adds, stating the benefits of the faceplates for diagnostics and maintenance. Alarm indication and parameterisation are also simplified by the RA Process Library.

By utilising a PlantPAx ready system as a higher-level process control system, a modern Smart Factory to produce brown glass
bottles and ampoules has been erected in France. It is intelligently and redundantly networked via EtherNet/IP and offers real-time visibility on all the currently running production processes. It is simple to expand and offers a wide range of connection options. Thanks to PlantPAx, all operating stations exhibit a uniform look and feel with standardised icons for visualisation purposes.

This reference project has entered operation as scheduled. “We generally want to ensure that our customers can get started with the plants supplied by us as soon as possible,” Ullrich concludes. “This is why we test all control systems in detail before they leave the company. We work with virtual production data, enter different recipes, produce thousands of batches and simulate an entire monthly production in order to avoid any ambiguities or errors in advance.”

Having passed these tests with flying colours it is no surprise that Ullrich is thinking of increasingly utilising this process automation solution in Zippe’s batch and cullet plants.

THE BOTTLE-MAKING PROCESS

The batch house is the initial location where raw glass material is housed in large silos before entering the glass furnace operations phase. After leaving the batch house, the mix is fed continuously into the furnace or tank where it is melted into glass. The glass depth must be controlled to within ±0.01 inch for proper forming machine operation.

Furnaces consist of three main parts, the melter, refiner and regenerators or checkers. Most furnaces are designed to use natural gas but can use alternate fuels-oil, propane and electricity if necessary. Furnaces range in size from about 450 to more than 1,400 square feet of melter surface.

A properly operated and well-maintained furnace will last for ten years or more with just one partial repair and will produce over 1,000 tons of glass per each square foot of melter surface over the life of the furnace.

The melter is a rectangular basin in which the actual melting and fining (seed removal) takes place. In a side-fired furnace, the batch is charged into the furnace through the doghouse, which is an extension of the melter, protruding from the back wall. Along each side of the melter, above glass level, are three to seven ports, which contain the natural gas burners and direct the combustion air and exhaust gases.

The melter basin is separated from the refiner by the bridge wall (throat end wall). Glass passes from the melter to the refiner through the throat, which is a water-cooled tunnel that extends through the bridge wall.

The refiner acts as a holding basin where the glass can cool to a uniform temperature before entering the forehearths. The melter and refiner are covered by crowns to contain the heat.

Feeder and delivery molten glass flows with the help of gravity from the refiner through the forehearth.

From there it is carefully cooled to a uniform temperature and viscosity prior to reaching the feeder. Using the pull of gravity, the hot glass flows through the orifice at the bottom of the feeder. Glass flow is controlled by the height of a ceramic tube in the feeder; a raised tube creates a heavy flow while a lowered tube results in a reduced flow. The glass flow undergoes a mixing action created by the rotation of the ceramic tube. This helps to make the temperature consistent while the downward motion of the plunger accelerates the glass flow.

This pumping action is timed with the shearing of the glass flow as it falls beneath the feeder to shape the falling gobs. After the gob has been sheared from the feeder it falls into a series of chutes where it is delivered to the blank mould on the Individual Section II machine. This is designed to ensure efficient production so that operators can take one or more sections out of production for repairs without shutting down production in other sections. Gobs enter the I.S. machine and are formed into containers through a process of controlled shaping and cooling of the glass. The total time needed to produce a container varies, but beer and soda bottles take approximately 10 seconds. Depending on the container’s size and shape, the machine’s production speed may be as fast as 700 containers per minute.

The materials used to make glass include approximately 70% sand along with a specific mixture of soda ash, limestone and other natural substances – depending on what properties are desired in the batch.
The expanding workplace

For smart meetings to be a reality, better communication tools are essential. The latest workplace technology innovations are already empowering people to be happier and more productive.

Many organisations are moving towards an agile workplace to increase employee wellbeing and cut operational costs by moving their staff to smaller, more cost-effective premises, encouraging hot-desking and remote working. We are seeing a widening of the definition of a workspace; from huddle and co-working spaces to coffee shops, more places are being deemed acceptable places to work, if the job gets done effectively.

Many of these changes have been facilitated by technology. The popularity of BYOD (Bring Your Own Device) has been driven by more powerful laptops, tablets and mobile devices, as well as better and increasingly ubiquitous Wi-Fi connectivity.

"With a fresh perspective driven by workspace environments and technology innovations we can start to see what the workplace of the future looks like, where technology improves collaboration between local and remote teams," Daniel Creigh, head of UK & I, Zoom Video Communications, says. "More importantly, we can start to paint a picture of what defines a smart meeting."

Welcome to a smart meeting

Companies are increasingly deploying video communications on a much bigger scale, with many of them introducing it to every single meeting room, desk and employee. "In part, this is in response to millennials coming into the workplace, who are used to consumer video applications and expect video-calling technology to be part of any modern office," Creigh says. "There is also an obvious shift towards mobile devices. This enables companies to allow every meeting to include remote video participants.

"An upside of this trend towards ubiquitous video communications is the increased flexibility it gives employees to work remotely without them feeling excluded from their office-based team, which is a factor that can boost productivity. In fact, a recent Forbes Insight survey found that 92 per cent of executives believe that the expanded use of video conferencing has a positive impact on their performance."

More importantly, the technology opens new ways for staff to feel connected and together as a whole company, even if satellite offices are in different cities or countries. This sense of community can be achieved by having screens in common areas at each location with a permanent video-call between them, enabling employees in separate offices to see each other every day, so they feel like they are in the same office. Companies are clearly seeing the value of this approach, as the same Forbes Insight Survey found that 80 per cent of executives now say that relative to audio conferencing, video conferencing is fast becoming the norm for internal teams.

Move to wireless

A second trend is the move towards wireless content sharing in meeting rooms, which is a development that is most welcome by those tired of walking into a room to discover the necessary dongles are missing or broken. It also gives meeting hosts and attendees the flexibility to move freely around the room.
“Audio conference calls are still common tools in the workplace, but they make it hard to stay focused, feel connected with the other participants, and be truly engaged in a call,” Creigh explains. “It’s likely that many people drift off mentally, don’t pay attention, or are tempted to check their emails during the call. It’s also hard to know who is listening or paying attention when you can’t see them. To further complicate matters, sharing a presentation often requires the use of a separate tool. There is now a growing trend to get rid of these different tools and consolidate them using a single tool for all types of meetings, whether it’s for audio conference calls, video calls, webinars, persistent chat, and/or sharing a presentation.”

The many uses for digital signage

TVs in meeting rooms and on office walls could be used in a smarter way when they are not in use. Workplace designers are increasingly drawn to the concept of ‘biophilic design’, which incorporates elements of nature in office design, such as plants, wood, blue and green colours, and natural light, which create a more harmonious environment that enables employees to feel more in-tune with nature and become more productive. By adding digital signage technology to all displays in the office, you can display biophilic images, such as waterfalls, forests and aquariums, in all meeting rooms and office spaces, to improve staff wellbeing and productivity. These same screens can also display informational content throughout your office, such as canteen menus, welcome messages, metrics, promotional videos, announcements, and more.

“Clearly, the workplace is evolving to a more agile environment, thanks to a new definition of the workspace and better communication tools,” Creigh concludes. “Few would dispute that smart meetings can keep staff happier, more connected, engaged, motivated, and more productive, a sure fire sign that technology is delivering on its promise.”

Daniel Creigh, head of UK & I, Zoom Video Communications

“WITH A FRESH PERSPECTIVE DRIVEN BY WORKSPACE ENVIRONMENTS AND TECHNOLOGY INNOVATIONS WE CAN START TO SEE WHAT THE WORKPLACE OF THE FUTURE LOOKS LIKE,”

CREIGH
To ensure maximum benefit from innovative industrial processes and technology, businesses need to consider IT innovation and become early adopters of pioneering brands.

IT has tremendous potential to transform businesses. From introducing new ways of working to using Big Data to provide transformational insights, it can radically change the way we run our organisations. However, many companies are slow to take the plunge into new IT solutions, creating a huge gap between the most IT-savvy firms and the IT laggards.

This has been studied by academics such as Harvard Business School professor Kristina Steffenson McElheren, who investigated why so many companies get it wrong. She believes IT has the potential to completely transform the supply side of business by flattening hierarchies, shrinking supply chains and speeding up communications. This enables organisations to spend more time thinking up new products and servicing customers, and less time checking boxes. However, organisations must be willing to engage in radical change to achieve the benefits, bringing together processes, people, organisational structures and supply chain partners. In her research into manufacturing firms, McElheren found that the larger firms were more likely to adopt incremental change, while smaller firms were more likely to adopt more radical change.

Fear of failure

Unfortunately, the aftermath of the 2008 financial crisis has made it more difficult to introduce IT innovation. “Finance directors are looking for rapid return on investment, the focus is on ‘business as usual’ rather than transformation, and in medium sized businesses, strategic thinkers have been driven out by continued restructuring,” Richard Blanford, managing director of IT infrastructure and consultancy company, Fordway, says. “Change programmes tend to be a response to external imperatives, such as new legislation, rather than being driven by a strategic vision. Meanwhile many organisations continue to use complex IT infrastructures that are no longer fit for purpose and are unwilling to make changes unless they are convinced that the alternative is substantially better.”
"Sometimes whole industries find that they have been left behind and find change is driven by necessity, rather than strategy. For example, the UK’s network of cash machines was based on the Windows XP operating system. When Microsoft withdrew support for this system, tens of thousands of cashpoints were still running it, leaving them potentially open to security breaches and putting immense pressure on the banks to implement a solution."

If organisations continue to do what they have always done, they cannot expect to achieve a different result. However, our willingness to innovate is also limited by learning at an early stage that good performance means avoiding failure, not making mistakes. Another academic, Edward D Hess, points out that this can limit our willingness to innovate because innovation requires a willingness to fail and learn. He believes that being smart is not about knowing all the answers but knowing what you do not know, prioritising what you need to know, and being very good at finding the best evidence-based answers.

The same premise is discussed by journalist Matthew Syed in his book, Black Box Thinking. He uses examples from the Mercedes Formula 1 team to Dyson to explain why success means confronting our mistakes and learning from them.

**Is IT meeting your business needs?**

“We find that many businesses are keen to adopt new ways of using IT but get bogged down in trying to understand the why and how before going ahead,” Blanford continues. “Instead, they need to step back and take a long hard look at how IT is meeting the needs of their business."

“The real value of IT to most organisations comes from three factors: the business specific applications and data to run their operations; the business process improvements that can be implemented more effectively using IT; and the information and insights that can be gained from the data the organisation retains. Anything else is just supporting infrastructure and systems, the ‘plumbing’ that keeps the business running but does not add strategic advantage.”

Blanford explains that the first step towards innovation is to review existing IT against these three requirements, and then think radically about what change could achieve. Business imperatives leave limited time for strategic thinking, so obtaining expert opinion from outside the organisation can help to provide the data on which to develop a business case for the board. Your organisation’s existing suppliers may not be best placed to do this, as they have a vested interest in maintaining the status quo.

“We recommend benchmarking against leading organisations, both in your own sector and elsewhere, studying analyst recommendations and talking to companies who have a track record in delivering IT changes in order to benefit from their experience,” he says. “We’ve all heard about hospitals learning from Formula One teams; what fresh expertise could be applied in your sector?"

“Sometimes an external point of view may be all that’s needed to ensure a change programme achieves the desired results. We worked with an organisation that was implementing a £1million IT improvement programme but was continuing to experience major reliability issues. We reviewed the various projects within their
programme and discovered that they were not designed to deliver specific business outcomes. For example, a project to install software which would warn of potential infrastructure problems had been completed and closed but the software was not being used, as the project brief had been solely about installation. With the problem identified, the various IT projects could be prioritised, and the in-house team were then able to complete the change programme successfully."

**Consider challenger brands**

Another important aspect of IT innovation is a willingness to consider challenger brands. Many organisations fear becoming an early adopter because they do not want to take what they perceive as a risk with an unknown vendor, no matter what innovative features their products offer or how competitive their price. As the saying goes, ‘nobody ever got fired for buying IBM’. There is also limited time to review market newcomers because today’s IT teams are much smaller.

However, by not considering up and coming vendors and new technologies, organisations miss out on opportunities to innovate, improve productivity and cut costs. "They also risk getting tied into their existing vendor's upgrade cycle, which can be expensive, may not take them along their desired path or, even worse, may promise new developments which then take longer than promised to materialise," Blanford explains. "Considering new market entrants and making a considered decision whether or not to change vendor should be part of the strategy for every organisation which is serious about using IT to gain business advantage. Is there an opportunity to do things better? Has the incumbent vendor kept up with market developments? Are there new solutions that offer better capability at reduced cost and/or with more flexibility, or has there been a step change in technology which is at the core of a new vendor’s product? It is important not to be complacent but to search out new and exciting products and then to choose the one which will really make a difference in a realistic timeframe.

"As a vendor independent company, we are constantly on the look-out for new products which can offer genuine business advantage, and there are some interesting options which are well worth considering. Some work in tandem with well-known products to improve performance, while others offer a new way of handling a need.

"A number of companies have found ways to help organisations get more from their Microsoft products. One such company is up and coming vendor Cireson, whose products will extend the capabilities of Microsoft’s system management software and will also help manage Microsoft licencing. Every organisation we have ever worked with has had licencing issues, so this or similar products could pay from themselves in licence savings alone. No vendor will ever tell you that you have spent too much on their licencing, so third party products have obvious advantages in this context.

"We have also been testing software from another challenger brand which enables organisations to improve the performance of their SQL Server database without adding more servers through enabling users to bypass the operating system when reading and writing data. If your users are complaining about slow response times and your database is a business-critical application, this could make a significant difference."

Another way to streamline and speed up IT performance is to reduce the amount of data stored and backed up. An article in a leading IT magazine claimed that an average document can be replicated 30-40 times, with copies stored each time as it is sent around. Deduplication has been with us for some time through established brands such as Commvault, IBM and Veritas, but there are also challenger brands such as Druva which will search endpoints and cloud locations; next generation storage from the likes of Tegile, SolidFire (now NetApp) and Reduxio which includes data compression and deduplication; and new ways of carrying out back-ups from Cloudian, Cohesity and Rubrik, which have progressed from emerging technology to challenger brand. As well as reducing the amount of data backed up, all will assist with GDPR compliance.

"Of course, it is vital to carry out a detailed evaluation before introducing new technology," Blanford concludes. "Before we offer any new product to our customers we carry out a comprehensive review, where we meet the companies concerned, trial their products and see how they stand up to a real-life environment. If everything goes well, they become part of our portfolio. It’s worth remembering that Google was once a challenger brand!

Change is always risky and IT change is extremely visible. If problems occur, there is no place to hide. But by asking the right questions, researching the options, learning from the best and not being afraid to innovate, organisations can achieve a step-change in performance.

**THERE IS A HUGE GAP BETWEEN THE MOST IT-SAVVY FIRMS AND THE IT LAGGARDS**
Arguably one of the biggest challenges facing UK businesses in the coming year is the continued confusion regarding access to Low Power Wide Area Networks (LPWANs) that are essential to support the deployment of IoT at scale.

At a time when organisations are being actively encouraged by the government to invest in innovation to drive up productivity, the continued prioritisation of broadband as a digital economy enabler is short-sighted. IoT is a technology that is set to deliver far more value than many of the high bandwidth applications can and the lack of availability is a concern.

All is not lost however. LPWAN roll out is a constantly changing situation, with both network standards and network deployments, licensed and unlicensed, still evolving. It is also a buyer’s market: there are several propositions ready that will enable organisations to leverage IoT and gain a competitive advantage. Here, we look at how it is the independent providers, able to provide access to a blended network model, who will enable not only IoT at scale today, but also provide a long-term solution that will drive new levels of efficiency and customer service.

**Competitive disadvantage**

“The state of IoT in the UK in 2018 is frustrating,” Nick Sacke, head of IoT and product, Comms365, says. “While industry giants are making huge investments in hardware, software and database platforms, as well as unlicensed networks, both low power networks LoRaWAN and SigFox, the under investment in cellular LPWAN in the UK is a concern. While progress in mainland Europe is patchy, with national LPWANs already in place across many countries, including the Netherlands and France,
and licensed cellular variants such as NB-IoT being rolled out across Eastern Europe, it is the unlicensed LPWANs, generally LoRaWAN, that are being rolled out fastest.”

In contrast, the UK is largely lagging: there is no cellular LPWAN (or NB-IoT) technology being rolled out in any shape or form and the unlicensed variant being rolled out by SigFox will not deliver end-to-end coverage before the end of 2018. Where, you may ask, are the UK network operators? “The answer, although not in the UK: Vodafone’s NB-IoT project, for example, is being piloted in Ireland and Spain, with no plans announced for any UK deployment as yet,” Sacke adds. “There is, therefore, a risk that companies will hang back on crucial IoT investment until this confusing situation is resolved.”

**Need to blend**

However, it is also fair to say that there is, as yet, no single global network that can support all IoT deployment requirements. From cost to scale and architecture, the level of market segmentation globally is creating huge challenges for organisations planning future developments – not least of IoT at scale across national borders.

“The problem is that with roll out of both licensed and unlicensed variants typically country by country, there is a clear need for cross-border roaming agreements, something that is only now beginning to be discussed,” Sacke explains. “So, what are the options for multi-national businesses that require a seamless, pan-country IoT deployment to achieve, for example, end-to-end cold chain tracking or seamless asset management across Europe? And how can UK businesses avoid lagging? To gain the benefits that IoT can deliver, a new model is required; one that can manage and blend several different networks, such as cellular and satellite – and agreements to achieve IoT at scale.”

But this is a constantly changing situation, with the evolution of both network standards and network deployments, both licensed and unlicensed. Given the potential longevity of these IoT deployments, it is essential to future proof as far as possible. How, for example, can an organisation achieve coverage without the IoT roaming agreements that have been standard in the cellular world for many years? How will the cost vary for different devices when connecting to a cellular versus a satellite network, or an LPWAN? What are the sensor options?

**Consultative approach**

Organisations need to embrace a consultative approach to understand the new complexity created by a blended network model. “Right now, there is a patchwork quilt of: no connectivity, some connectivity and full connectivity,” Sacke says. “To achieve full coverage, companies must invest in multiple networks to achieve a seamless solution. Plus, with many projects set to last five to ten years, it is essential to avoid tie-in to specific networks.

“To address this issue, sensor manufacturers are now creating hybrid devices that support more than one network, for example LoraWAN and cellular, giving companies the chance to move onto a new network as it is rolled out, rather than face expensive retrofitting of devices. Hybrid software gateways are also being developed, offering organisations a chance to support multiple networks. There is a cost implication, but options are evolving to enable organisations to deploy IoT at scale across a blended network.

“What has become very clear over the past few months is that successful IoT deployment now demands a robust ecosystem of expert companies, including sensor manufacturers and service providers, working together to drive both standards and best practice deployment methodology across a blended network model. This ecosystem needs
 WHAT IS LPWAN?

Low-power WAN (LPWAN) is a wireless wide area network technology that interconnects low-bandwidth, battery-powered devices with low bit rates over long ranges. LPWAN is not a single technology, but a group of various low-power, wide area network technologies that take many shapes and forms. LPWANs can use licensed or unlicensed frequencies and include proprietary or open standard options. Created for machine-to-machine (M2M) and internet of things (IoT) networks, LPWANs operate at a lower cost with greater power efficiency than traditional mobile networks. They are also able to support a greater number of connected devices over a larger area.

 WHAT IS LORAWAN?

The LoRa Alliance promotes its Long-Range WAN (LoRaWAN) protocol as an open global standard. According to the Alliance, LoRaWAN could provide coverage for entire cities or even countries with just a few base stations.

 WHAT IS SIGFOX?

The proprietary, unlicensed Sigfox is one of the most widely deployed LPWANs today. Running over a public network in the 868 MHz or 902 MHz bands, the ultra-narrowband technology only allows a single operator per country. While it can deliver messages over distances of 30-50 km in rural areas, 3-10 km in urban settings and up to 1,000 km in line-of-site applications, its packet size is limited to 150 messages of 12 bytes per day. Downlink packets are smaller, limited to four messages of 8 bytes per day. Sending data back to endpoints can also be prone to interference.

 WHAT IS NB-IOT?

Narrowband-IoT (NB-IoT) and LTE-M are both 3rd Generation Partnership Project (3GPP) standards that operate on the licensed spectrum. While they have similar performance to other standards, they operate on existing cellular infrastructure, allowing service providers to quickly add cellular IoT connectivity to their service portfolios.

NB-IoT, also known as CAT-NB1, operates on existing LTE and Global System for Mobile (GSM) infrastructure. It offers uplink and downlink rates of around 200 Kbps, using only 200 kHz of available bandwidth.
Joining the dots

CTS looks at how manufacturers are integrating, correlating and analysing real-time operational data to help them to deliver on just-in-time strategies.

Traditionally, the value chain involved in turning raw resources into physical goods runs on data. Smart factories are at the forefront of the latest industrial revolution, where connected devices and automation enable data-based decisions that optimise production.

The maturity of sensors; wireless connectivity; AI, cloud and edge computing have played a large part in enabling this latest industrial revolution. Today, sensors can be embedded into most equipment components, collecting and transmitting large volumes of data without disrupting their function. Battery life has improved to the point where replacement does not constitute a maintenance issue. Sensors can reliably and unobtrusively monitor everything within a manufacturing operation, from the extraction of raw materials, to the delivery of processed goods.

Data assets

The first step in the Industry 4.0 value chain starts with data capture. “The more integrated the various data streams and the higher the quality of the data, the more valuable this raw resource becomes as an input in the analytical process,” Dr Rado Kotorov, chief innovation officer at Information Builders, explains. “Hence, integration, data quality and master data management technologies have emerged as the new tools to manage and enrich data assets.”

The PriceWaterhouseCooper (PwC) report, ‘2017 Industrial Manufacturing Trends,’ highlights the benefits of gaining insights from operational data. PwC advises that industrial manufacturers need to mine operational data by investing in, ‘connectivity tools that provide insight into production levels, inventory and capacity availability, quality levels, and order status from all their suppliers’.

According to Gartner and other analyst groups, the digital enterprise technology platform will comprise five core interrelated systems: IoT/device management; analytics and decision support management; employee/processes management; customer relationships and partnership management. Naturally, there are going to be a variety of different technologies within each system, but a key feature of this new architecture is that the systems are interrelated with a business intelligence system at the core.

Improving visibility

Industry 4.0 sensors act as the eyes and ears of the manufacturing process, converting physical stimuli, such as dimensions, vibration, light, moisture, or chemical contamination into electrical pulses. “A continuous stream of operational data provides shop floor employees and management teams with real-time visibility into the status of machines, products, production lines, warehouse conditions and logistics operations,” Kotorov adds. “Finding patterns in IoT data is important. Commercial IoT initiatives, and Big Data projects in general, also involve importing, integrating, profiling and contextualising data.”

Integration of data streams from a
variety of sources can be used to build a picture of the entire operation from raw material to customer delivery and used to support real-time decision making. For example, machine-to-machine (M2M) data can help predict when parts will need to be replaced and alert when machines require recalibration; helping to combat waste and improve efficiency.

Data visualisation

Kotorov explains that while everyone can benefit from the information gleaned from machine sensors, qualified data scientists are in short supply. Therefore, intelligent, timely decision-making can be supported by providing employees with intuitive InfoApps, with graphics that clearly convey the status of production lines, stock levels, warehouse conditions and delivery schedules.

Learning to be lean

Timely, trusted data helps to achieve lean manufacturing goals. A culture of continuous improvement can be achieved by driving operational efficiency and agility by minimising standing inventory; improving flow; removing waste; partnering with suppliers and responding to change.

“Machine-to-machine (M2M) technologies that share operational data are a natural fit with the production environment,” Kotorov says. “Data from supervisory control and data acquisition (SCADA) and manufacturing execution systems (MES) provide managers and operational staff on the factory floor with reliable information on which to base strategic and tactical decisions.

“In addition to helping employees to take data-based decisions, Industry 4.0 involves the automation of M2M communication and decision making. This automation offers the dual benefit of speeding up processes and reducing errors and associated costs.”

RFID technology already supports efficient material handling, warehouse management and shipment tracking. The integration of IoT technologies now gives manufacturers even greater visibility. “These capabilities enable logistics to be optimised to reduce costs, as well as calculating the date and time of deliveries.

Dr Rado Kotorov, chief innovation officer at Information Builders
more reliably to improve the customer experience,” Kotorov continues. “This opens up new sources of revenue for some organisations, such as shipping companies that are able to sell container tracking data to customers in the form of InfoApps.

“Smart factories are able to use cyber-physical systems to monitor processes and respond to changes at the local level, while feeding data back to the central system to provide management teams with full visibility of the status of machinery, goods and logistics networks.”

**Implementing AI**

In its Top 10 Strategic Technology Trends of 2018, Gartner has predicted that artificial intelligence will become a foundation component of all services. The manufacturing sector was an early adopter of AI technology and this is set to increase exponentially as manufacturing powerhouses increase industrial automation.

The International Federation of Robotics (IFR) reported that globally there was an average of 74 robots per 10,000 employees. South Korea leads the world in automation, with 631 robots per 10,000 employees, followed by Singapore (488), Germany (309), Japan (303), Sweden (223), Denmark (211), the USA (189), Italy (185), Belgium (184) and Taiwan with 177 robots per 10,000 employees. The UK is ranked 22nd in the world for robot density, with 71 units per 10,000 employees.

China, currently ranked 23rd by the IFR, has an ambition to become one of the world’s most automated nations by 2020. Its robot density almost trebled in the three years to 2016 and it is on target to increase to 150 units per 10,000 employees in the next two years.

Dark factories highlight data’s value

While the automotive and electronics industries are leading the adoption of automated manufacturing systems, other industries are also recognising the cost efficiency and productivity gains of operating smart and dark factories. Last
year, Amazon, which employs 200,000 people, increased its automated workforce by 50 per cent and now has 45,000 robots working across 20 order-fulfilment centres.

“Amazon’s robot army is now larger than the Netherlands’ actual army,” comments emerging trend strategist, Matthew Carr, in The Oxford Club’s Investment U. Highlighting the efficiency gains of the robot revolution, Carr reports: “A study by Deutsche Bank estimates that Amazon’s Kiva robots reduce expense by 20 per cent - or $22 million – per warehouse.”

Data quality

The PwC report, ‘Industry 4.0: building the digital enterprise’, states that ‘Data analytics and digital trust are the foundation of Industry 4.0’.

Data must be managed as a key asset to add value to goods and services. We have unprecedented opportunities to use operational data to connect the dots across the entire value chain. Operational information can be immediately presented to employees for decision making in real time. The instantaneous flow of information creates transparency in the operations that in turn drive faster and more efficient operations.

Machine-generated data is generally more accurate because it is not subject to data entry errors. However, Industry 4.0 involves the integration of a plethora of data sources to build a complete picture of the manufacturing value chain. Therefore, it is crucial that data is automatically cleansed, so that everyone (including the robotic workforce) is working from trusted data.

Valuable data

In this latest industrial revolution, data has itself become a valuable resource that can be mined, refined and monetised by providing organisations with new opportunities to identify and eliminate inefficiencies. By facilitating automation and enabling everyone within the supply chain to act upon the latest information, organisations are better able to compete locally and internationally.

While automation heralds the inevitable speculation around the redundancy of traditional manufacturing roles, there will always be a requirement for human oversight, creativity and initiative. Using robots to take on repetitive and physically risky tasks also has the potential to increase the wellbeing of human employees.

INDUSTRY 4.0 IN ACTION: DATA FEEDS AVOID FOOD WASTE

Lipari Foods delivers 150 truckloads of groceries to 8,000 customers over an 800-mile area. Any delays in the warehouse or on the road can accumulate throughout the night, resulting in late deliveries and spoiled food.

“Supply chain data has evolved to more than just transactional data from an ERP or WMS system,” Joe Beydoun, director, SCM/business intelligence, Lipari Foods, LLC, comments. “Today, in 2018, we have various data sources that we capture, collect, and react to in a near real-time state.”

Lipari combined IoT data and analytics to optimise the layout and slotting of more than 22,000 stock keeping units in its state-of-the-art warehouse. Delivery vehicle telematics data was combined with inventory updates and real-time performance measures from warehouse equipment.

Actionable KPIs are displayed on dashboards and exception-based reports are automatically distributed when activities fall outside of typical parameters, helping Lipari to spot and quickly address potential errors in orders and shipments. Additionally, Lipari Foods used its data-based insights to optimise a warehouse, eliminating the need for costly expansion.
Why collaboration is key to digitisation success

CTS looks at how automation and robotics are transforming manufacturing processes into more intelligent approaches, with technology filling the gap in strategic capabilities as manufacturers strive to create a nimble, yet capable infrastructure.

Manufacturers have entered an era where the ability to quickly respond to changing market conditions is a prerequisite for success.

It is an era where consumers have potentially thousands of options they may choose for a new vehicle and make-to-order is the preferred method of manufacturing. In this scenario, the need for employees with specialist skills and intelligent, flexible factories, could be the difference between operating efficiently and falling further behind more agile competitors.

“For solutions relating to safety, fuel emissions and connectivity, the innovation content in new vehicles is around 90 per cent. OEMs are also endeavouring to reduce fuel consumption and, in this context, focusing on new, lightweight materials. As early as the vehicle design stage, these materials need to be conceived for ease of repair and maintenance, but provision must also be made for an increasing number of electronic components.”

A further challenge is the personalisation of vehicles with the aim of manufacturing products in a batch size of one, for the same cost as a mass-produced vehicle. While the vehicle user benefits from these new technical possibilities, they result in a completely new process environment for automotive manufacturers and suppliers.

Such challenges are shifting the focus of automotive manufacturers, who are no longer reliant on traditional production managers to oversee plant maintenance, instead handing greater responsibility to CFOs, IT directors, operational directors and heads of digital transformation. At the heart of the solution is the convergence of technologies known as Industry 4.0, comprising cyber-physical systems, the Internet of Things, cloud networks and cognitive computing. While such technologies are becoming relatively accessible to all, maintaining and optimising them requires an ongoing collaborative approach.

Smart factories call for smarter services

For smart factories to operate seamlessly, connected systems must be continually updated and improved and this is where it pays to collaborate. “Leadec works with several automotive OEMs behind the scenes of their intelligent factories, observing the drivers of the new digital era, in which self-learning and digitally networked systems are increasingly expanding the capabilities of production and value creation,” Glaser-Gallion says. “To help manufacturers meet demands of customers, we connect the various drivers: new
concepts for automation, digital data and analysis, networked systems and platforms, sensors, new approaches to human-machine interaction, mobile solutions and visualisation technologies. Such trends are helping IT directors to enable the production line to increasingly personalise vehicles, while making the manufacturing process more productive.

“Earlier this year a well-known German manufacturer asked us to support the pre-implementation of new technologies, working with its own management team during the planning phase of a new factory - and it is this type of collaboration that is essential for technology projects of this sort to be effective.”

Whether it is a question of procuring new production facilities or modernising existing infrastructure, intelligent factories are increasingly being designed with technology and production efficiency at the forefront. And it is the role of the IT director and specialist maintenance experts to assume responsibility for the reliable functioning and availability of machines and processes from the point of installation.

As smart factories have evolved, so too has the definition of site maintenance. Today, such a term encompasses the planning and project maintenance of all services at the plant, customised organisational models, the implementation and supervision of all technical and administrative procedures through to inspection, servicing and maintenance, and the ongoing improvement of machines, systems, and processes. To ensure that production systems are flexible, available and reliable, and that logistical procedures run smoothly, IT directors need to make use of existing technologies and at the same time develop their own solutions to optimise internal workflows.

“We've worked in many manufacturing organisations where customised software solutions have been developed for controlling production, logistics and materials, because the linking of sensors and actuators both in the product and the plant infrastructure continually changes maintenance measures,” Glaser-Gallion adds. “By collecting, using and evaluating real-time performance data systematically, IT directors can better plan and optimise activities, making it easier to predict maintenance fluctuations and plan production schedules accordingly.

“By collaborating with specialists to manage this process, information systems can be effectively linked with portable devices and then operated and maintained externally. The challenge businesses face is that often compatibility of information systems and IT interfaces differ greatly from customer to customer. The systematic monitoring of technologies and applications in real-time can help overcome this and prepare IT directors for the next contract that needs to be integrated into their own digital systems.”

**Smarter people**

A more collaborative approach to digitisation has benefits beyond the customer data transaction; it also plays a role in future skills development. Just as manufacturers need to ensure their customers receive a seamless service without disruption, their digital systems also need to provide this level of reassurance to production teams. For this to be possible, the data analysis requires human interpretation and skilled, competent individuals that can scrutinise live data and use it to their advantage.

Thus, a comprehensive understanding of robotics and automation is required. “It is often the case when collaborating with external partners, that they already have their own training courses that employees can take advantage of,” Glaser-Gallion concludes. “Indeed, Leadecc has its own education centre, which provides both internal and external training programmes in robotics and automation. This enables us to help our customers train their own specialists by providing short-term, needs-based professional training. We have even created an accredited, advanced training programme in robotics, based on our customer's requirements.

“This blend of skills development, training and customised digitisation services is an attractive proposition to manufacturing IT directors who have enough of a job ensuring that their connected technologies work today, without worrying if they will continue to function seamlessly tomorrow. As the transformation of automotive production continues to be steered by industrial services, collaborative partnerships between internal teams and external experts is crucial to ensuring digitisation success during the age of the fourth industrial revolution.”

**“By collecting, using and evaluating real-time performance data systematically, IT directors can better plan and optimise activities,”**

---

**Markus Glaser-Gallion, CEO of Leadecc Group**
As industry continues to encompass data analytics, artificial intelligence and other disruptive technologies, edge computing will became a vital tool in the IT armoury.

Edge computing is now a fundamental tenet of IT infrastructure, it is literally pushing boundaries by redefining today’s modern data centre. Forward thinking organisations are always looking to progress by utilising the latest technology developments, and as part of this, we are seeing a move towards Artificial Intelligence (AI) and the Internet of Things (IoT) to gain data driven insights. However, it’s important that the underpinning IT infrastructure can support new applications and still forms a critical part of the business strategy. So how can organisations modernise their data centres and take the next step in today’s digital transformation?

Jason Collier, founder at Scale Computing explains that a key component to transforming the data centre is edge computing, as it offers a unique way to work to take advantage of the benefits around AI and IoT. “Although the term is new, the concept has been around for a while as it encompasses the needs of many remote and branch offices,” he says. “As a broad definition, edge computing can be defined as computing that takes place outside of the typical data centre, meaning IT infrastructure is closer to where the data is created and used. Many smaller, remote locations such as hospitals, trains, ships, manufacturing facilities, retail organisations, and oil rigs have operated in this way for a long time. However, the rise in AI and IoT has created a new and fresh demand in a way that will allow organisations to gain quicker and faster data insights.”

“Cloud, IoT, and edge computing all have very real and critical roles to play in both modern and future IT infrastructure,” Collier
As data-driven applications grow, there is a demand for speed and instant access to information, this is what will give organisations that competitive edge. “By utilising edge computing and bringing data closer to the source there is a noticeable impact in performance and speed,” Collier adds. “Traditional data centres are often far away from IoT and AI devices, and although cloud computing bridges this gap in terms of distance, it relies on a good connection and can often come with latency challenges. Edge computing eliminates this by providing on-site micro data centres, where data is analysed and stored on the individual device. By analysing data at the edge of the network, organisations can deliver the real-time performance these applications need.”

The cloud has already changed the way organisations work and the role of the data centre, but it will not fully replace the need for on-premises IT. “We are still discovering how the rise of IoT and AI will consume cloud computing and on-site data centres as organisations are still at the start of their journey,” Collier continues. “But, the need for modern on-premises data centres that can help organisations to utilise the benefits is apparent. The cloud has many benefits, especially scalability and elasticity, however, when it comes to real-time fast insight without latency, the cloud also has its drawbacks. Take for example IoT devices in remote locations, without a strong internet connection, sending and retrieving information will come with latency challenges.”

As IoT and AI applications grow, and we start to demand faster and quicker insights, edge computing will become more important. For example, as we head into the digital transformation and start to encounter smart cities and driverless cars, these will require continuous data insight and fast performance. Organisations that are prepared now and have the infrastructure in place to support these performance driven applications will be ahead of the curve in utilising the benefits. “Micro data centres are a big part of fulfilling this need,” Collier says. “It is essentially a data centre scaled down to operate on site and suit a specific business model. For these applications that require more fine-tuned performance and speed, local on-premises computing resources can meet the demand. An edge computing strategy may well encompass some cloud element, but it will certainly include on-premises IT.”

“Cloud, IoT, and edge computing all have very real and critical roles to play in both modern and future IT infrastructure,” Collier concludes. “While their roles will continue to evolve, each is a growing part of the IT industry and hybrid IT infrastructures that adopt and combine these different technologies will have a competitive advantage over those that do not. Just as these technologies continue to evolve, so will the ways they’ll continue to intersect.”

JASON COLLIER, FOUNDER AT SCALE COMPUTING
Leading the way in Industry 4.0

Connected Technology Solutions spoke to Martyn Williams, managing director of industrial software provider, COPA-DATA UK, about what is needed to achieve Britain’s goal of becoming an Industry 4.0 leader in 2018.

Where are we at on the road to Industry 4.0?
First came the dawn of mechanical machines, succeeded by the introduction of electricity, quickly followed by the third industrial era, the advent of computers and the internet. Now, as we enter the so-called fourth industrial revolution, Industry 4.0 is moving from buzzword to reality.

In 2018, the manufacturing industry will see a higher adoption of industrial digital technologies (IDTs), think robotics, intelligent automation software and additive manufacturing. These technologies have been available for a while, but greater accessibility means they are no longer out-of-reach for small to medium-sized manufacturers.

What is helping to drive this growth?
According to the Annual Manufacturing Report 2017, the majority of manufacturers believe that increased connectivity in their facilities will help to increase their productivity. However, the benefits of IDTs are even greater when replicated on a national scale. Increasing Britain’s output will assist in the country’s worldwide competitiveness, strengthening supply chains and, ultimately, strengthening the UK as a world leader in industrial digitalisation.

What are the challenges that the UK faces to become a true leader?
The country’s engineering skills shortage has been a hot topic of conversation for a while, but only recently is the industry recognising the importance of increasing innovation, rather than just high investment. One of the recommendations of the government’s review on industrial digitisation, Made Smarter, is to create a national Skills Strategy to identify the skills requirements in the UK. However, this will only work in tandem with investments that will encourage innovative behaviour.

By nature, engineers want to design, invent and create things.

What about the perceived threat to jobs from Industry 4.0?
The increase in digitalisation on the factory floor has been widely criticised for removing the need for human intervention and, therefore, removing the need for highly-skilled engineers — but this view is misguided.

Digitalisation provides an opportunity for engineers to move away from the menial, repetitive jobs that automation can manage. Instead, engineers must begin to use their expertise and talent for defining and leading the strategies and processes needed for such a high level of automation.

Do we need a bottom-up or top-down approach to succeed?
For Britain to become a pioneer of industrial technologies, the country needs inspiring leadership, but management is not just about maintaining authority. Positive leadership requires a divestment of power by giving employees the authority to make decisions.

Consider this. A machine operator in a factory is arguably the best qualified person to make decisions about a particular piece of equipment. Despite this, the decision to repair or replace a machine is often passed to C-level. Our world view limits the way we think and skews our understanding of the wider picture. But, to make the best decisions, the authority must be shared with those that are most informed.

How would you sum up the UK’s future direction?
It is our responsibility to create the next generation of leaders, these are our apprentices, graduates and machine operators. However, as Britain’s industrial landscape is changing so quickly, we cannot simply create replications of ourselves. As the factory of the future continues to adapt, our future leaders need to get used to taking ownership of important business decisions.

To become a pioneer of industrial digitalisation, Britain’s manufacturers need to invest in technology, encourage innovation and inspire the next generation. Britain may have been the first country to industrialise during the early 19th century, but, today, it has the potential to become a global leader of the next industrial era.

Connected Technology Solutions spoke to Martyn Williams, managing director of industrial software provider, COPA-DATA UK, about what is needed to achieve Britain’s goal of becoming an Industry 4.0 leader in 2018.
CTS is the leading source of authoritative and engaging information for all managers within the industrial arena
To get your own copy of CTS please visit www.connectedtechnolgysolutions.co.uk
You Can’t Fake It in the Field

ServiceMax from GE Digital is the premier field service management platform for equipment maintenance and managing your assets.

We are the only complete field service software solution helping companies perfect service delivery, drive revenue and growth, and delight customers. Learn why ServiceMax is the proven leader in Field Service Management.

Visit us online at www.servicemax.com or call us at +44 203 846 7320.

We are field born, field tested.

“With ServiceMax at the hub of our global service transformation, we will also be able to launch new service offerings in line with our customer needs and expectations with better market penetration.”

Marel - ServiceMax Customer

Learn more about our customers’ success by joining a European event near you!

servicemax.com/uk/servicemax-workshop-series-2018