Connected industry

euautomation

At times, it feels like we cannot escape the innovations of smart technology. Televisions, smartphones, fridges and believe it or not, even meals.

Farmers are using connected technology to monitor soil conditions and assess the health of livestock. In-home smart cookers have the ability to alert you at the exact moment your yorkshire puddings have reached optimum crispiness and once you have finished your meal, your wearable fitbit will be there to give you a prompt reminder of how many steps you will need to take to burn it all off.

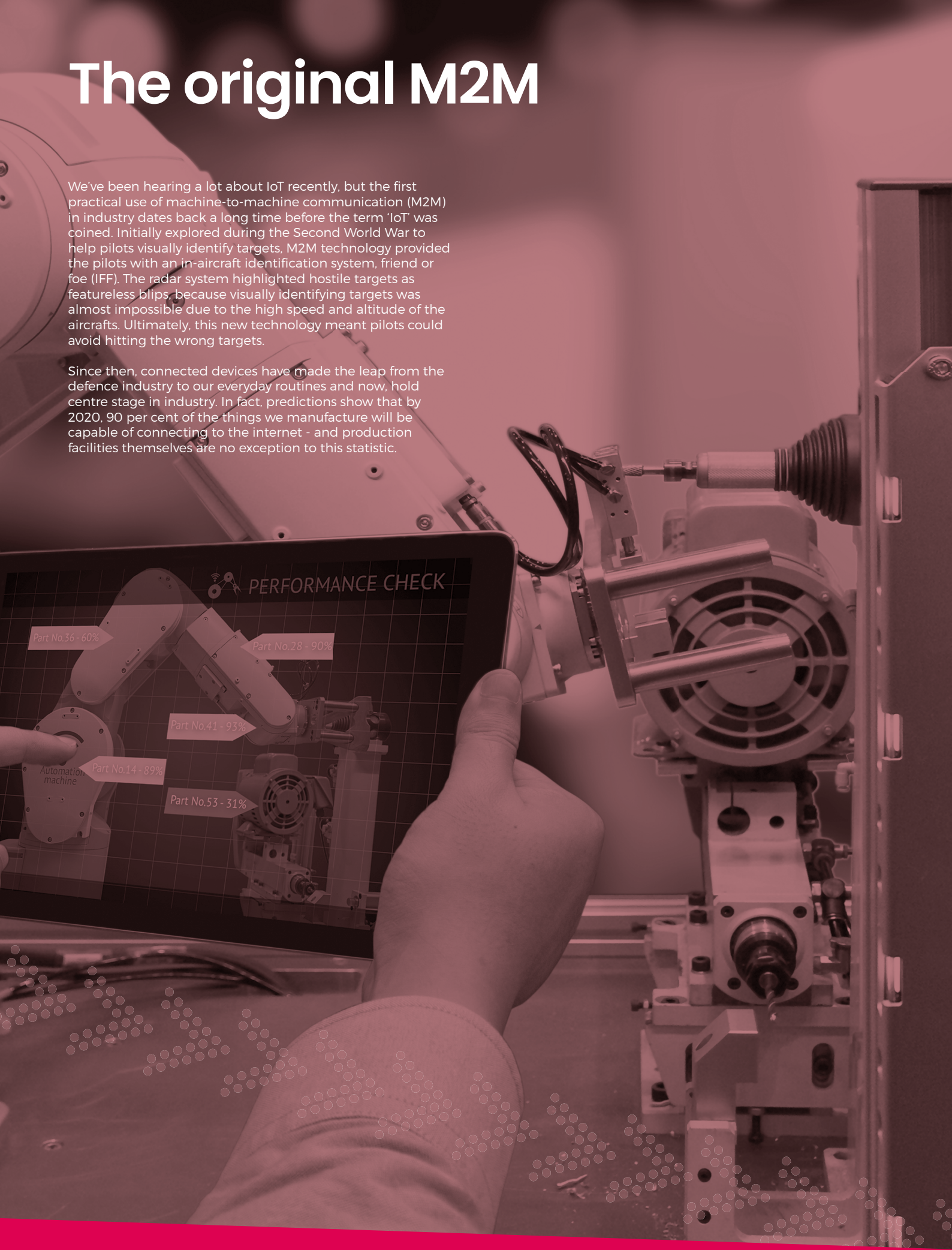
While it is easy to take these small changes for granted, our familiarity with smart technologies proves how quickly we have adapted to a new, connected age.

Homes are becoming more intelligent, as smart meters allow homeowners to access and manage their utilities and energy consumption more effectively. City councils do the same by monitoring the infrastructure of their newly integrated smart cities, supervising traffic, pollution and transport - all at the push of a button. Without doubt, the Internet of Things (IoT) has changed the way we live. Consumers have taken up interconnected technology with a remarkable degree of adaptability, but when it comes to industry, the transition has been significantly slower. In this special report, we look at the latest developments in machine to machine (M2M) communication and the potential they hold for industry.

The original M2M

We've been hearing a lot about IoT recently, but the first practical use of machine-to-machine communication (M2M) in industry dates back a long time before the term 'IoT' was coined. Initially explored during the Second World War to help pilots visually identify targets, M2M technology provided the pilots with an in-aircraft identification system, friend or foe (IFF). The radar system highlighted hostile targets as featureless blips, because visually identifying targets was almost impossible due to the high speed and altitude of the aircrafts. Ultimately, this new technology meant pilots could avoid hitting the wrong targets.

Since then, connected devices have made the leap from the defence industry to our everyday routines and now, hold centre stage in industry. In fact, predictions show that by 2020, 90 per cent of the things we manufacture will be capable of connecting to the internet - and production facilities themselves are no exception to this statistic.

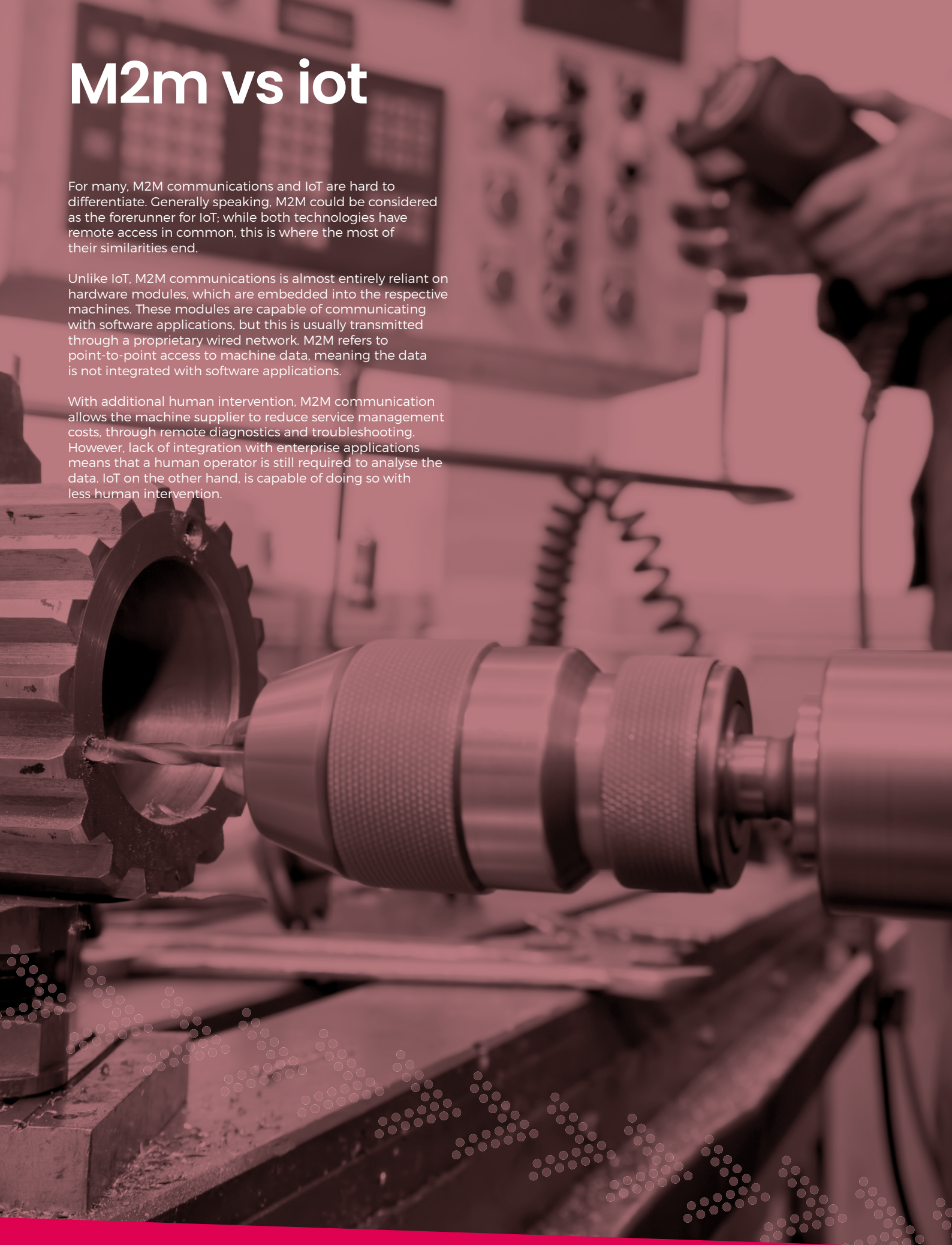


M2m vs iot

For many, M2M communications and IoT are hard to differentiate. Generally speaking, M2M could be considered as the forerunner for IoT; while both technologies have remote access in common, this is where the most of their similarities end.

Unlike IoT, M2M communications is almost entirely reliant on hardware modules, which are embedded into the respective machines. These modules are capable of communicating with software applications, but this is usually transmitted through a proprietary wired network. M2M refers to point-to-point access to machine data, meaning the data is not integrated with software applications.

With additional human intervention, M2M communication allows the machine supplier to reduce service management costs, through remote diagnostics and troubleshooting. However, lack of integration with enterprise applications means that a human operator is still required to analyse the data. IoT on the other hand, is capable of doing so with less human intervention.



What exactly is a “Thing”?

There have been visions of a worldwide network of interconnected objects even before the global computer network launched almost fifty years ago. Despite this, there remains confusion about what the term IoT actually means. According to market research giant Gartner, the definition of IoT is, ‘a network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment’. While Gartner’s definition makes sense, it doesn’t really delve into the nuts and bolts of how IoT works.

A connected ‘thing’ must be a uniquely identifiable device with its own IP address. The device - whether it is a surveillance camera, wearable technology, a smart meter or an industrial component - is capable of connecting over a network to share and receive data. While IoT can be wireless, it doesn’t necessarily have to be connected via WiFi. A network can be anything from 2G/3G/4G, a wired network, ZigBee, Ethernet or even good old Bluetooth.

Embedded with sensors, the device is able to “speak” to other components within the system. For example, in a food manufacturing plant processing jars of cranberry sauce, the conveyer belt transporting the fruit through a cleaning process should be able to communicate with the machine separating the cranberries into set portions. This ensures any irregularities or blockages in the batch are dealt with in advance. Further down the line, machinery used to measure the mass of fruit will communicate this weight data to the packaging machines.

These processes are not new to manufacturing. The basic processes of transporting, washing and packaging, have always been present in the food industry. The difference is that today, human workers are not required to perform these menial tasks. As the costs of industrial standard smart sensors continue to fall, automated production is slowly but surely becoming standard industrial practice.

Enter the smart factory

In industry, IoT has made its impact on almost every sector. For manufacturers and utility providers, connected devices have dramatically transformed the way industrial facilities operate. Since the introduction of six axis robotic arms to the automotive production lines of the 1960s, manufacturers of all types have been looking for ways to automate their processes and machines. Today, industry is in agreement that to thrive, the modernisation of manufacturing facilities is essential.

Already, many manufacturers have implemented some form of industrial automation, using M2M communication to aid operations, increase efficiency and lower costs. Nevertheless, the more recent introduction of IoT marks the next major transformation in industrial operations. According to a report by market analyst firm Berg Insight, the number of installed and active wireless devices in industrial automation reached a whopping 10.3 million in 2014. By 2020, this figure is expected to reach 43.5 million.

The benefits of connected technology in industry are clear. By using smart sensors to measure operating parameters, manufacturers can collect valuable production data. Temperature, speed, productivity, energy efficiency and any other information deemed relevant to the organisation is gathered and sent to a remote controller. From there, this smart technology enables automatic adjustments to machinery on the shop floor - ensuring production levels remain efficient and productive.

For organisations requiring precise operations, namely heavily regulated sectors, such as pharmaceutical, food, beverage, oil and gas, this lack of human intervention can have huge benefits. Leaving less room for human error and producing a more reliable data trail, automated operations are the obvious choice for seamless production.
That being said, the introduction of automated production lines is bound to cause anxiety for workers in the industry. In recent years, we have been bombarded with media coverage tarnishing the rise of smart machinery, artificial intelligence and industrial robotics as the final nail in the coffin for employees of manufacturing plants. However, industry reports and predictions show this is not the case.

Human obsolescence

Throughout history, technology has created thousands of new jobs while eliminating old ones. As recently as the first half of the twentieth century, a huge percentage of Londoners were limited to working in manufacturing and heavy industry. Today, while much of the heavy industry has moved away from London, the city has transformed into a booming hotspot for the services sector.

The most obvious trait of an IoT-enabled factory is machines being able to communicate and perform actions without much need for human intervention. However, this doesn't render humans' roles obsolete. Inevitably, some will argue the introduction of new technology has led to a rapid decline in heavy industry and, to some extent, this is true. However, by eliminating menial tasks, workers in the manufacturing industry are free to take on roles that require human skills like innovation, creativity and judgement, skills industrial automation cannot replicate.

Aside from the irrational fear of an AI takeover, there are some concerns about M2M technology that are entirely justified. The most important risk factor of M2M is security, particularly for newer wireless M2M networks.

Cutting wires

Traditionally, M2M technology has used a wired infrastructure. However, for industries characterised by remote and inaccessible facilities, like the oil and gas industry, wireless M2M technology remains one of the few viable options. In fact, wireless M2M has become so popular that a network has been specifically designed for the technology - 6LoWPAN (IPv6 over low power wireless personal area networks). Reliant on wireless connectivity, oil and gas operatives can use 6LoWPAN technology to remotely monitor and control the performance of inaccessible equipment such as tanks, water meters, pumps and valves.

The majority of today's consumer internet is based on its predecessor IPv4 (internet protocol version four). As a new technology, 6LoWPAN uses the newer IPv6 (internet protocol version six). The earlier IPv4 allowed space for around 4.2 billion unique IP addresses, but in 2011 this capacity proved insufficient and IPv4 addresses were exhausted. In contrast, IPv6 holds space for a much larger number of IP addresses, enough for the internet to grow for decades to come. Considering the predictions for both IoT growth and wireless M2M advancements, this larger capacity for IP addresses will prove necessary in coming years.

Securing the Smart factory

Fears surrounding this increase in wireless connectivity are inevitable and as a result, organisations across all industries are taking extra steps to secure their smart factories.

For the healthcare sector in particular, there is no denying advancements in connectivity have made exceptional and positive changes. Already, M2M is being used to supplement patient treatment through remote monitoring and communication, whilst keeping track of vulnerable patients as they move through a healthcare facility. However, just as at-home wireless network can easily be infiltrated and hacked, M2M devices carry some level of risk.

On a wider scale, organisations across all industries should be cautious before implementing M2M communication. Manufacturers must understand M2M and the cyber security risks it involves to take the necessary measures to protect their facilities against any attacks. Let's face it, even the most complex of M2M-enabled systems are still vulnerable to challenges of user identification and authentication, causing anxiety about data access and fears of losing confidential company information.

To avoid these risks, organisations are turning to intelligent automation software, embedded with complex security measures to secure their smart factories and industrial environments. By preparing supervisory control and data acquisition (SCADA) systems for the potential cyber threats and external vulnerabilities of industrial connectivity, organisations are placing security at the top of their priorities.

Unrelated to security, another risk of implementing M2M or IoT is the lack of maturity of the technology. While we've been hearing a lot about connected industry, both IoT and wireless M2M technology are still in the early stages of implementation, meaning universal standards are yet to be established.

For manufacturers, industrial connectivity can generate benefits including lower labour costs, a reduction in human error and increased levels of production and efficiency. However, the technology doesn't come without its challenges. To successfully implement this technology in an industrial facility, organisations should address these challenges before making the move to connectivity.