Achieving excellence in a complicated IIoT constellation

Updating operations to support a universe of internet-connected things comes with an array of challenges. How, where (and why) should you start? Fleur Doidge reports.

Manufacturers forging an Industrial Internet of Things (IIoT) constellation to drive myriad elements of productivity, visibility and efficiency often seek to adapt older or more traditional equipment in the process. However, Graham Upton, Chief Architect, Intelligent Industry, Capgemini, confirms that many struggle to get the desired results despite successful proofs-of-concept – and not just because the tech isn’t always compatible.

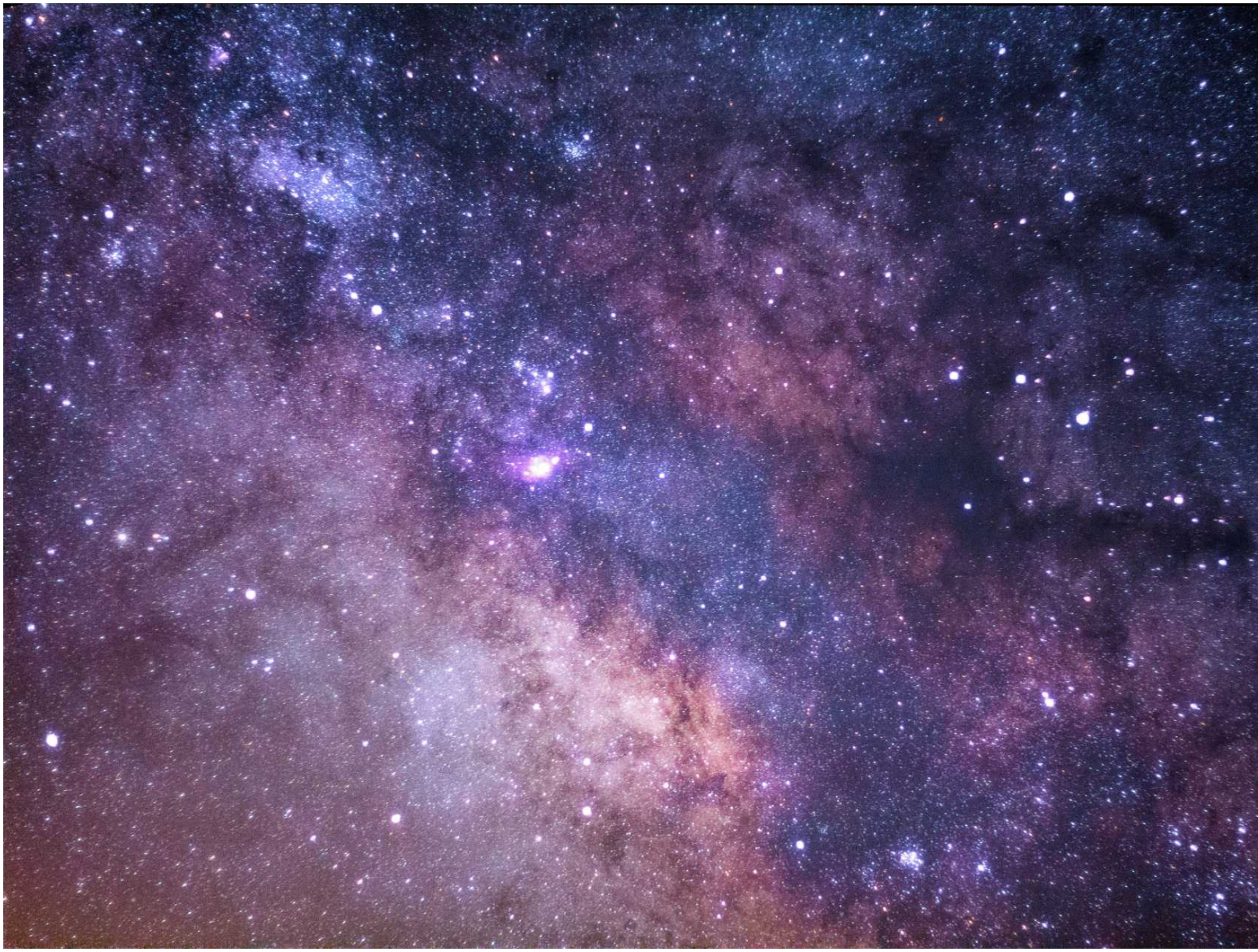


Image courtesy of Jeremy Thomas/ Unsplash

IIoT enablement might well drive performance and machine visibility but when scaling up and out, problems emerge. Often, they haven't fully developed the business case, he says. "Everybody forgets there's the human factor to learn as well," Upton adds. For instance, he has seen staff simply file their IoT-connected iPads or other devices in a drawer and ignore them, sticking to traditional ways that have worked previously.

That means manufacturers should focus from the start on fully understanding and scoping the whole picture, Upton says – how management, people and processes, data handling considerations and tech aspects down to networking and physical layout work together.

First things first

Then proceed incrementally, says Mark Hughes, Regional Vice President at ERP software vendor Epicor. “First ask: what will drive the most value if I enable it with IIoT and why?” he adds. “One aspect that could be easy is starting to monitor energy usage, potentially down to the machine cell level. What will it achieve unless we can drive a reduction in use – maybe powering down unused or idle machines?”

Older machines might be connected if they can support interface boards, or additional hardware devices might be inserted to show activity, warnings or status.

Parts can be tracked as they move off a conveyor, boxes scanned during packing, and people traced between locations. At a more advanced stage, you might consider building a digital twin, enabling real-time modelling for data-driven insights.

“Take your asset register of machines and establish which ones will already publish tags that can be used to get visibility into their operating parameters. For machines that are not connected, review manufacturer options or look to add your own programmable logic controllers (PLCs) and sensors to

capture what you need," says Hughes.

Avoid it where it will add no value: if you have a machine or process that is efficient enough, it will not add a benefit to be feeding back data." Today, feeding the right data to the cloud and allowing for stream-based processing means machine learning can be applied even at remote or 'edge' parts of the network.

But when everything is connected, security becomes critical. Paul Baird, Chief Technical Security Officer at IT security firm Qualys, explains that connecting old, capital-expensive operational technology (OT) assets can be especially risky – with OT security about ten years behind IT security – and sometimes OT cannot be patched due to 24/7 operation.

Meanwhile, ransomware attacks on operation networks have spurred cyber insurance providers to tighten policies and mandate proactive cyber security practices, processes and risk management. "Attempting to force a retrofit to get data in and out is the wrong approach," warns Baird. "Plan and phase in any transformation projects over time. This is the safest way of protecting your environment and keeping your organisation running."

Consider defence in depth

Baird recommends "defence in depth" locking down, preventing in-bound connections from unknown locations or IP addresses when sensor data is published to an IT application or service. If it's interacting with other services or uses application programming interfaces (APIs), follow Open Web Application Security Project (OWASP) guidance.

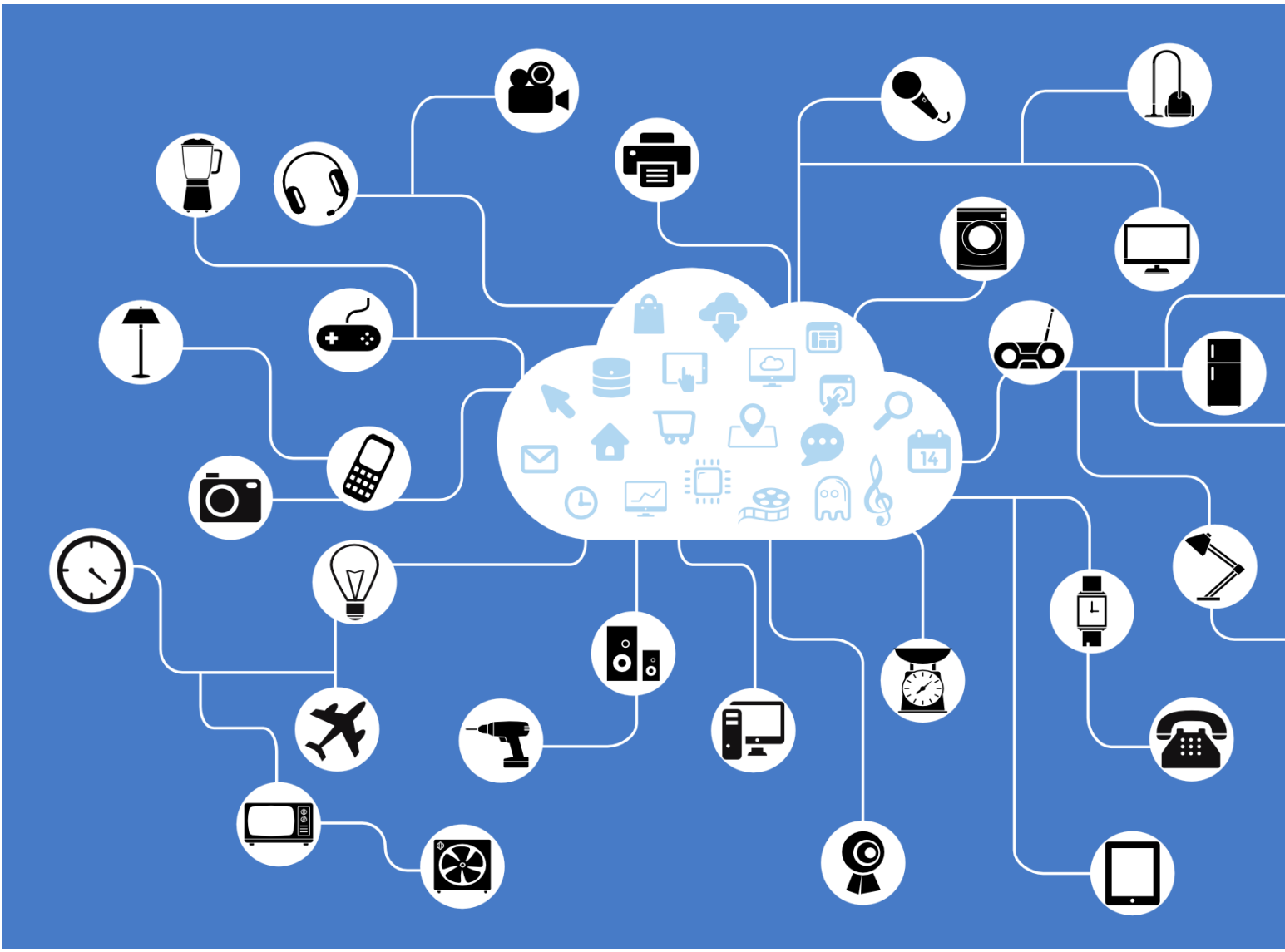
Sachin Shah, Chief Technical Officer at security firm Armis, says most are at a "transition" point

somewhere along the road to full IIoT benefits. On a factory floor, there are so many degrees of difficulties on the connector system that you need to understand the legacy environment already there.

Ideally a smart factory would start with a greenfield, brand-new physical construction, which isn't realistic, he says. Get a solid understanding of both IT and OT, from mechanical instrumentation and controls, chemicals and electrical skills to internet and IT. By understanding the components of appropriate data analytics and insights, including data lake and log management, with all the related services, success moves within reach.

"You need lots of analysis and qualifying before translating into IIoT systems," Shah says. "As soon as you bring in a wireless capability, does it have any conflicting frequency that can stop my other processes, chemical systems or life safety systems? These are things you need to worry about." Martyn Crew, Director of Solutions Marketing at IT networking specialist Gigamon, reiterates that its not just about spending on the right technology, which can be expensive.

Look at well-established IIoT best practice models for technology implementations within an existing framework – such as the Purdue Model for structuring a network. He also suggests investigating retrofit "IoTin-a-box" type kits. Bolted on to take over communications from that machine to the network, they can improve visibility, including scanning for security risks or vulnerabilities opening up on a particular device.



“You need visibility across everything to ensure security and overall application performance,” Crew says. “But you also need encapsulation – make sure that if, for example, an older machine on the shop floor gets hacked, that hack cannot spread across the network.” He adds that to mitigate against upfront costs, focus on your most vulnerable machines first. That way, you may have the best chance of optimising performance out of an investment in machine upgrades.

Why bother with IIoT challenges?

Phil Beecher, CEO and President of standards lobby group Wi-SUN Alliance, says that environment and security issues can also be eased by IIoT enablement – even though disruptions can be exploited if cyber security is not sufficiently robust.

“For example, in hazardous environments, IIoT can be used to keep staff safe and help ensure consistency in the production process,” Beecher argues. “Manufacturing and process automation has been around for many years, but IoT is standardising connectivity and data sharing for greater flexibility.”IIoT enablement can improve manufacturing security, ensuring raw material quality and grade or end product is fit for purpose, or improving integrity and safety – for instance by monitoring for cross-contamination in food manufacturing facilities.

“Certificate-based sensor security with firmware signing means software updates, whether outsourced or in-house, can be monitored and validated – reducing the risk of malware (malicious software) attacks,” Beecher says. Lee Jones, Head of Manufacturer Solutions at connected-construction software provider National Building Specification (NBS), adds that IIoT enablement boosts the value of Product Information Management (PIM) systems.

Manufacturers have typically held information in many different places, whether development information, manufacturing information, warranty information, or details of different businesses. “One of the most beneficial things I think a manufacturer can do is look at structuring the product information internally,” Jones says.

“If they can maintain their data in this one single source of truth, whether implementing stage gates for new products introduced or just maintaining information.” Simon Carr, General Manager at consultancy Industry Forum, says a downside is that manufacturers may “overly relax” with plentiful IIoT measurements to hand and not engage in the same level of proactive and preventive maintenance as a result. “Will your IIoT adaptations detect a lack of cleanliness, or poor lubrication, or a lack of alignment in the machinery? Mostly not, yet these factors heavily influence the lifespan. Total Productive Maintenance (TPM) principles still apply,” Carr says. Manufacturers should be wary of overreliance on “shiny” digital enhancements that produce graphs and other visualisations on their smartphones or wherever. Staff must still be trained and educated to correctly use the information and software involved, he points out.

A few are getting IIoT right

Currently, Carr suggests, maybe only five or ten of every 100 manufacturers is “doing IIoT” in a value-adding way. “Just monitoring the condition doesn’t do anything,” Carr adds. “And companies are often under pressure, and it’s probably worse now than ever, with maybe a few people on the shop floor to run and maintain equipment.”

Peter Ruffley, CEO at data analytics software company Zizo, adds that complex API development can be needed to get to the data or deploy new sensors to give the whole picture. “Even some IIoT enabled devices or machines do not make it easy to get the data needed for analysis – stuck in or behind bespoke or difficult to use pieces of software designed by the manufacturer themselves,” Ruffley notes. Extracting useful data from older IT can involve “highly proprietary” ERP or MRP systems; data from older systems and devices may not even be in an easily usable format, Ruffley adds.

Roy Clarke, Solutions Consultant at PTC, adds that the oldest kit might be a mystery to your current team: situations evolve from when a machine was initially commissioned and installed. Modern machines typically have PLCs running the machine code and performing operations. However, attention must be paid to multiple factors, from specific processes used by the technologies, standards and protocols that ensure tech is generally compatible, he says.

Image courtesy of Greg Rakozy/ Unsplash

“Modern PLCs will have separate boards for processing natural control functions and for input/output; older PLCs might just have words – you obviously don’t want to be hitting that and potentially impacting control operations, for example.” Consider constraining effective data capture when retrofitting, especially when PLC access isn’t easy or possible: ask if you really need all those specific data points and try to limit how much data you collect and process. Look closely at what you already have, and maybe speak to partners you already work with that know your operation already for guidance, Clarke says.

“I’ve had conversations with customers who have PLCs but zero knowledge of what is going on in there and how to collect data hence retrofitting sensors plus gateways is the only way,” he says. “And it’s a crowded space, with plenty of vendors offering three main components for retrofitting mainly legacy assets for IIoT.” Rob Russell, CTO and Co-Founder at predictive-maintenance software

company Senseye, confirms that ease of implementation has become a larger barrier for smaller organisations than the technology itself.

“Ask what’s actually causing downtime and maintenance costs in your business? Go and assess that. From there, we’ll figure out what data we need and the sensing technology,” Russell says. “We see some machines that the customer finds very complicated and doesn’t quite understand themselves, with complicated processes associated to them.”

Ask for help if needed

It can make sense to get original equipment manufacturer (OEM) advice on things like sensor placement, especially with smaller manufacturers that might have fewer established architectures and ways of doing things. “There’s a world of decisions to be made,” Russell says. “Actually, partnering, maybe with a systems integrator, can support you with the right type of experience in that area.”

Ben Johnson, CEO of IT solution provider BML Digital, agrees that connectivity – physical network infrastructure with “robust, highly available WiFi” – and security are two of the largest challenges that often aren’t adequately addressed. “It’s not complicated to add monitoring that can be surfaced through dashboards with thresholds for alerting and so on,” he says.

The next big challenge is to actually automate those amendments. That’s a big step without human intervention. Manufacturers need a lot of data to be confident that the changes can be made without human say-so, Johnson points out. Initial stages of IIoT enablement can be expensive but offer little ROI – which makes some businesses reluctant to spend enough to get to the latter, more profitable stages of IIoT, he adds. “Particularly if they’ve been promised the moon in the past with IT investments.”

Tor Mackenzie, Consultant and Founder at Manufacturing Advisory Directorate (MAD) Yorkshire agrees that manufacturers must first fully scope out the challenges they want to resolve and the results they want to achieve via the technology. Buy-in from top management down is needed. “It can sometimes simply be left to the IT department to initiate the project and make it happen,” Mackenzie points out. “And there’s no one-size-fits-all.”

Key takeaways

* Scope out the entire business case in all aspects before you begin

* Ensure you fully understand current status and scope out where you want to be in the future before embarking on an IIoT enablement project

* Key technical challenges include connectivity, security and automation – while maintaining required operational parameters

* Installing the specific tech can be the easy part. Ensuring that all working parts fit together and that the human elements have been addressed is critical to success.

* Do not leave IoT simply to the IT department; make sure you have buy-in at all levels of your organisation

---

While we're on the subject of Industrial Data, why not sign up for our Industrial Data Summit? Taking place in Birmingham at the end of April.

Source: **Achieving excellence in a complicated IIoT constellation**