Issue 2 2026

INDUSTRIAL NEWS



TOMORROW STARTS TODAY

LAYING THE FOUNDATION FOR TOMORROW'S DATA-DRIVEN OPERATIONS

ALSO IN THIS ISSUE

AUTOMATION: FROM SKILLS SHORTAGE TO SKILLS EVOLUTION

CONTROL: HOW INFRASTRUCTURE MANAGEMENT IS EVOLVING







Editor
Jon Hughes
jon@industrialnews.co.uk

Design
2b Media

Partnerships
Jenn Blakesley
jenn@industrialnews.co.uk

The statements and opinions expressed in Industrial News are not those of the editor or the publication, unless described as such.

Copyright in the contents of Industrial News, its sub-brand magazines, Industrial Views special reports, its website and newsletters is the property of the publisher. The publisher and the sponsors of the magazine are not responsible for the results of any actions or omissions taken on the basis of information contained within this publication.

Industrial News is a controlled circulation journal, published monthly and based in Birmingham, UK.

Circulation: ~33,000 average
Period: Jan 1st 2026 – June 1st 2026

2b Publishing

CONTENTS

INTRODUCTION

Breaking the cycle of deferred modernisation 4

IN THE NEWS 6

AUTOMATION

Innovation and trust in the next era of manufacturing 12

From skills shortage to skills evolution 16

FOOD

Is it time for food innovation to catch up to GLP-1s? 20

DATA & ANALYTICS

Why ERP has become a competitive necessity for UK distributors 24

Upgrading legacy platforms for next generation connectivity 26

Industrial AI won't scale without solid data foundations 30

Physical AI needs a trusted layer 32

AI is redesigning industrial connectivity. The network has to evolve with it. 36

POWER

How planning reform could help secure the UK's industrial energy 40

From green claims to proven performance 42

CONTROL SYSTEMS

From SCADA to web-based control platforms: how infrastructure management is changing 44

ELECTRONICS

Security by design 46

IN CONVERSATION

Rob Demain, e2e-assure 48

Nick Leeder, ITI Group 54

Kurt Markley, Apricorn 58

Paul DellaVilla, CCT 62



BREAKING THE CYCLE OF DEFERRED MODERNISATION

Industry has spent years discussing what the factory of the future will contain. AI, autonomous systems, connected assets, predictive maintenance, digital twins, and software-defined production have all taken their turn at the centre of that conversation.

Just as predictably, those discussions are punctuated by the voices of engineering managers pointing to the challenges already impeding operations today: ageing equipment, fragmented data, constrained power, skills shortages, insecure networks, and systems that were never designed to work together.

It is a familiar cycle. New capabilities emerge, the same operational obstacles are restated, and the more difficult foundational work is deferred to another budget period. With each passing year, that pattern becomes harder to justify.

The challenges themselves are not new. What has changed, however, is the pressure surrounding them.

Manufacturers are being asked to raise productivity, strengthen supply chains, reduce emissions, improve energy efficiency, manage growing cyber risk, and make practical use of AI, often while working with tighter capital, limited specialist skills, and infrastructure that is already under strain.

That combination makes this as pivotal a moment as any to establish the foundations of a more resilient industrial future.

Those foundations are rarely the most exciting part of modernisation. They are found in reliable data, interoperable systems, secure connectivity, dependable control, skilled people, and the ability to upgrade operations without destabilising production. They also extend beyond the factory gate, into the planning, energy, and network infrastructure on which industrial growth increasingly depends.



There will always be a reason to delay this work. Production cannot stop. Legacy equipment still functions, however imperfectly, and that level of continuity can present a short-term reassurance that is threatened by change. Integration introduces risk, budgets remain contested, and thus the immediate operational problem will usually take priority over the strategic one.

None of those realities is likely to disappear by itself. Nor will another wave of technology compensate for foundations that remain weak.

A more resilient industrial future must be built through the accumulated decisions to repair, connect, secure, and strengthen the systems industry already relies upon.

Tomorrow starts today. That means the groundwork must too.

— Jon Hughes, Editor

INDUSTRY

SCHNEIDER ELECTRIC LAUNCHES AUTOMATION MODERNISATION SERVICE

Schneider Electric has launched Industrial Automation Modernization as a Service, a new offering designed to help manufacturers update automation systems without interrupting production.

The service combines Schneider Electric's EcoStruxure Automation Expert software, lifecycle services, and automation expertise with HPE SimpliVity hybrid cloud infrastructure. It is intended to give industrial operators a software-defined route to modernisation while continuing to run existing PLC and DCS assets.

The companies position the model as an alternative to large rip-and-replace programmes, allowing users to shift automation investment from capital expenditure to operating expenditure and upgrade systems incrementally. Schneider says the approach addresses common barriers around proprietary control architectures, cyber resilience, ageing assets, and shortages of specialist automation skills.

The offer is built on open automation principles, with both Schneider Electric and HPE involved in UniversalAutomation.org, the industry initiative promoting software-defined automation based on IEC 61499. HPE's role is to provide the resilient compute, storage, and data protection layer needed to support mission-critical operational workloads from edge to cloud.

INDUSTRY-SPECIFIC AI COMES TO EUROPEAN MANUFACTURING

Epicor has launched Epicor Prism across the UK and selected European markets, extending its AI-driven ERP strategy for manufacturers and supply chain businesses.

Embedded directly in Epicor Kinetic, Prism gives users conversational access to live ERP data, documents, spreadsheets, PDFs, and related operational information without requiring specialist analytics skills or separate AI tools. The launch forms part of Epicor's Cognitive ERP strategy, which aims to move ERP from passive systems of record towards software that supports real-time decision-making.

The portfolio includes more than 18 pre-built AI agents designed for industry-specific workflows across manufacturing, distribution, building supply, retail, and automotive. These can help users interpret MRP logs, identify supply and fulfilment risks, analyse carrier performance, extract and validate documents, and support less experienced staff inside ERP environments.

The rollout comes as manufacturers face pressure to improve productivity, strengthen supply chain resilience, and make better use of operational data despite persistent skills shortages.

Epicor says Prism respects customers' existing governance and role-based security, with actions remaining subject to human oversight. The company also claims Prism Developer for App Studio can reduce the time needed to build and test ERP screen customisations by an average of 60%.

INDUSTRIAL ROBOT SHIPMENTS FORECAST TO REACH 760,000 BY 2030

Global industrial robot shipments are forecast to rise from 549,555 units in 2025 to 761,303 units in 2030, according to new research from **Interact Analysis**.

The market intelligence company said the sector returned to growth in 2025, with shipments increasing by 5.1% after a 2% contraction in 2024. Over the 2025–2030 period, shipments are expected to grow at an average annual rate of 6.7%, supported by stronger market sentiment, reshoring activity in the US, and demand from semiconductor, electronics, logistics, and new energy applications.

Material handling and assembly are expected to be among the main application areas driving adoption, with forecast compound annual growth rates of 7.0% and 6.9% respectively. The figures point to continued automation investment in logistics operations and precision manufacturing-line assembly, where manufacturers are seeking higher throughput, repeatability, and labour resilience.

Growth will be uneven across regions. APAC is projected to record the strongest shipment growth among the major markets, with an average annual growth rate of 7.1% from 2025 to 2030. This compares with 6.2% for the Americas and 4.7% for EMEA.

Interact Analysis said weak automotive investment is constraining growth in EMEA, where industrial robot shipments contracted by 4.9% in 2025. High interest rates have reduced the number of new automation projects in the region, affecting demand for high-end welding and heavy-payload robots. Automotive will nevertheless remain the largest sector for industrial robots globally, with shipments forecast to rise from 171,556 units in 2025 to 223,864 units in 2030.

At country level, India is expected to deliver the highest growth, at 12.5% across the forecast period. Germany is forecast to achieve a much slower compound growth rate of 3.7% between 2025 and 2030, with shipments predicted to contract by 0.3% in 2026.

Collaborative robots are set to be the fastest-growing robot type, with shipments forecast to increase at an average annual rate of 17.4% between 2025 and 2030. Articulated robots will remain the largest segment, but their growth is forecast at a more modest 5.0%, while SCARA robots are expected to grow by 5.9%, supported by electronics and semiconductor demand.



MICROCHIP ADDS DSPIC33CK VALUE LINE DSCS

Microchip Technology has introduced its dsPIC33CK Value Line family of Digital Signal Controllers, targeting cost-sensitive real-time control applications that need deterministic performance without excessive peripheral overhead.

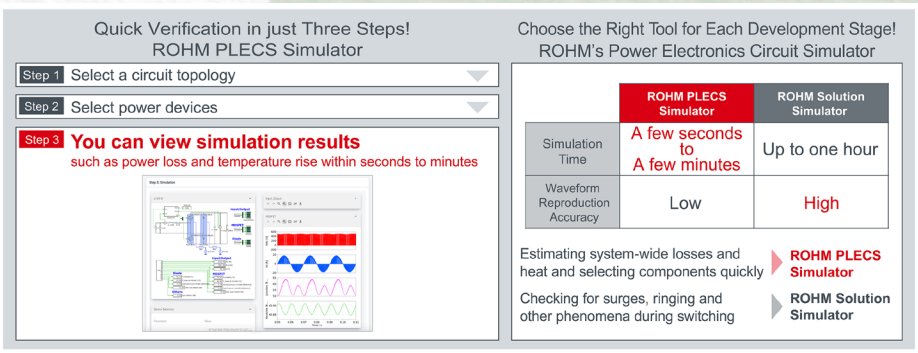
The devices combine up to 100MHz processing, high-resolution pulse-width modulation, and a 12-bit analogue-to-digital converter to support motor field-oriented control, touch interfaces, and precision sensing. Microchip said the range is intended for designs where engineers need dependable control capability, reduced complexity, and predictable device cost.

The family integrates peripherals that can consolidate multiple system functions onto a single device, helping reduce external component count, PCB footprint, and bill-of-materials cost. Flash memory options range from 32KB to 256KB, with compatibility across the broader dsPIC33CK family to support future migration.

The devices offer up to 2ns PWM resolution across eight channels, a 12-bit ADC supporting up to 2MSPS, on-chip analogue comparators with a 12-bit DAC, and communications support including CAN FD, LIN, SENT, UART, SPI, and I²C.

Automotive-grade reliability, including AEC-Q100 Grade 1 qualification, is supported alongside security features for secure boot and firmware updates. Development support includes a dsPIC33CK Value Line Curiosity Nano evaluation kit, Motor Control DIM, and compatibility with Microchip's MPLAB ecosystem.

ROHM LAUNCHES PLECS-BASED SIMULATION TOOL



ROHM has released the ROHM PLECS Simulator, an online tool designed to help power electronics and system designers carry out rapid circuit verification using ROHM power devices.

Available through ROHM's website, the simulator is based on PLECS simulation software and focuses on loss and thermal calculations during the early stages of circuit design. Users can select a power electronics topology and ROHM device models to simulate power loss and temperature rise in seconds or minutes, reducing the time normally required for early device selection.

The tool launches with 20 circuit topologies, with ROHM planning to expand supported device models and topologies, including SiC devices, IGBTs, and power modules. It is intended to complement the existing ROHM Solution Simulator, which provides more detailed waveform verification using high-precision SPICE models.

ROHM said the two tools will allow engineers to move from early loss and thermal checks through to detailed circuit validation.

Registration is required, but access is free.

FOOD PROCESSING

METTLER-TOLEDO EXPANDS X6 X-RAY INSPECTION RANGE



Mettler-Toledo has launched the X56 DXD+ dual energy photon-counting x-ray system, expanding its X6 Series for packaged food inspection.

The system is designed to detect difficult low-density contaminants, including rubber and plastics, in medium and large packaged products on single lanes, or smaller packs across multiple lanes. Typical applications include pet food, crisps, potatoes, multi-packs, and bulkier cartons where variable density, overlapping textures, or high-contrast product formats can challenge conventional single energy systems.

The X56 DXD+ combines DXD+ detector technology with Advanced Material Discrimination Pro software and AI capabilities to improve inspection reliability while reducing unnecessary product rejection. It also supports completeness checks, clip detection, and product trapped in seal inspection.

Designed for high-speed production, the system offers throughput of up to 500 products per minute, tool-free belt removal, hygienic construction, flexible reject options, and traceability through image recording or integration with Mettler-Toledo's ProdX data management software.

PRISM DELIVERS RECYCLABLE DAIRY SLEEVING FOR BIO&ME

Prism eLogistics has developed a fully recyclable shrink-sleeve packaging solution for Bio&Me's new functional kefir drinks, which the companies say is a first for the dairy category.

The range uses clear bottles covered with EcoFloat shrink sleeving, rather than conventional white dairy plastic and standard labels. EcoFloat is engineered to support sink-float separation and can be recycled through established polypropylene recycling streams, allowing both the bottle and decoration to be recycled.

The sleeve also provides the opacity needed for dairy safety requirements while avoiding coloured plastic, which can be harder to recycle and may attract higher Extended Producer Responsibility fees. For Bio&Me, the format also increases brandable space, giving the product a full-bottle design and more room for consumer information.



Prism said the project shows recyclable shrink sleeving can support regulatory compliance, on-shelf impact, and lower packaging-related environmental burden for food manufacturers moving away from coloured plastics.

POWER

SHORELINE WIND AND YOUWIND INTEGRATE PLANNING PLATFORMS

Shoreline Wind and **YouWind** have announced a strategic partnership and product integration intended to provide an end-to-end digital planning workflow for wind farm development.

The collaboration connects Youwind's cloud-based platform for early-stage onshore, offshore, and battery energy storage project development with Shoreline Wind's AI-powered simulation and optimisation software for wind farm design, construction, and maintenance. The companies said the integration will create a continuous digital trace from site screening, layout design, yield modelling, and technical evaluation through to construction planning, operational go-live, and computerised maintenance management systems.

The aim is to reduce the fragmentation that often occurs between front-end project engineering and long-term asset operation. Wind farm layouts, hybrid wind and storage configurations, expected yield data, and technical assessments developed in Youwind can now be migrated into Shoreline's platform without losing key project data. In return, Youwind users can draw on Shoreline-modelled turbine availability and expected operating expenditure data to strengthen early-stage yield assessments and business cases.

The integration is intended to support both new wind projects and repowering strategies for existing assets, where more accurate design, cost, and operational modelling can improve investment decisions before construction begins.

Shoreline Wind and Youwind said they have worked with shared customers to refine the integration around real engineering workflows. For developers and operators, the value lies less in another software layer than in removing a familiar handover problem: project data that has to be rebuilt each time a wind farm moves from planning to delivery.



CONSTRUCTION

MEDITE SMARTPLY INVESTS €75M IN CLONMEL MDF SITE



MEDITE SMARTPLY has announced a €75 million investment programme at its Clonmel MDF manufacturing facility, marking 50 years of the MEDITE brand and reinforcing its long-term commitment to panel production in Ireland.

The programme centres on replacement and renewal of the site's existing biomass boiler system, alongside upgrades to fuel handling, dryer systems, and associated production infrastructure. The Clonmel facility operates continuously and produces around 400,000m³ of MDF products each year, with the boiler system providing the thermal energy needed to dry wood fibre during panel production.

"MEDITE has been a long-standing part of the Clonmel community, and this investment – the largest current investment in MDF production in Western Europe – reflects our intention to continue manufacturing here long into the future," said Neil Foot, CEO of MEDITE SMARTPLY.

MEDITE SMARTPLY said the investment will strengthen process control, improve plant reliability, reduce downtime, and support consistent product quality across its continuous manufacturing lines. Dieffenbacher and Sunds Fibertech are among the European technology suppliers involved in the project, which will modernise energy generation, fuel handling, and fibre drying operations.

The project has secured planning consent through Ireland's Strategic Infrastructure Development process and includes provisions covering environmental protection, waste management, water supply, and ecological monitoring. The upgraded infrastructure is intended to help the site respond to increasing operational and regulatory requirements while supporting supply resilience for customers across UK, Irish, and European construction and interiors markets.

By moving fully to renewable biomass as the primary heat source, the new system will eliminate natural gas use at the site and reduce fossil fuel-related Scope 1 carbon emissions.

INNOVATION AND TRUST IN THE NEXT ERA OF MANUFACTURING

*By Falc Borchard, President Sales & Applications North America, **PIA Automation***

Manufacturers are entering a phase in which innovation is no longer defined by product development alone. In highly regulated industries, new devices must not only be developed faster, but also produced reliably, validated transparently and scaled under tightly controlled conditions. Automation, robotics, AI-supported methods and digital production data are therefore becoming central to how manufacturers bring new technologies from concept to market.

For many years, automation was often introduced once a product design had matured, and production volumes justified the investment. Today, that sequence is changing. Manufacturers increasingly have to consider automation much earlier in the product lifecycle, as production rarely remains static. A device may move from prototyping to clinical or pilot production, then into ramp-up and eventually full-scale manufacturing. Decisions made early in that journey can have a significant impact on how quickly, consistently and economically production can be scaled later.

At the same time, regulatory expectations continue to rise. Authorities are placing greater emphasis on transparency, traceability and accountability, particularly as software, data-driven functions and AI-supported systems become more relevant to product performance and production quality. Traditional validation remains essential, especially where physical evidence, real-world data and documented process control are required. However, digital and AI-based methods are increasingly being used to complement these approaches. They can support preliminary analyses, help identify risks earlier and allow manufacturers to focus validation activities more efficiently.

For manufacturers, this means compliance can no longer be treated as a final checkpoint. Quality, cybersecurity, data governance and process control must be embedded into development and production from the beginning. Innovation creates value only when it can be reproduced, documented and trusted.



AUTOMATION AS A FOUNDATION FOR SCALABLE INNOVATION

Automation is no longer limited to efficiency gains. It increasingly determines how reliably new products can move from development to scalable production. Early-stage manufacturing requires flexibility, fast adaptation and the ability to handle lower volumes. Later stages require repeatability, stable output and consistent quality. The challenge is to design production environments that can support both.

Flexible automation platforms help bridge this gap. They allow manufacturers to establish controlled processes at smaller scales and then expand toward higher-volume production with fewer redesign efforts. This can shorten time to market, reduce technical risk and support regulatory alignment across the product lifecycle.

Equally important, automation creates consistency at scale. Standardized processes reduce manual variability and help ensure that each device meets defined quality and safety requirements, regardless of where or when it is produced. In medical and life science manufacturing, where repeatability can directly affect patient outcomes, this level of process control is essential.

Modern production systems also generate valuable data. Digital records, process parameters and quality information strengthen traceability, simplify audits and support continuous improvement. When used effectively, production data becomes more than documentation. It becomes a tool for improving design, manufacturing performance and long-term product reliability.

THE EXPANDING ROLE OF AI

AI is rapidly becoming a driving force across the manufacturing ecosystem, but its greatest value often lies in supporting better decisions rather than replacing established processes. In engineering and production, AI-supported methods can help analyze complex datasets, identify patterns and detect potential weaknesses earlier in the development cycle.

> INNOVATION CREATES VALUE ONLY WHEN IT CAN BE REPRODUCED, DOCUMENTED AND TRUSTED.

Simulation-based approaches such as virtual commissioning (VC) also allow manufacturers to evaluate system behavior, process sequences, material flows and production scenarios before extensive physical testing begins. This can reduce unnecessary iteration, support validation and help teams better understand how manufacturing systems may perform under different conditions.

On the shop floor, robotics and AI-supported systems are enabling more adaptive production environments. Robots are no longer limited to highly repetitive tasks in rigid layouts. Increasingly, they are used in flexible systems that can respond to product variants, changing production volumes and complex handling requirements.

As AI adoption grows, so do the responsibilities. Data privacy, algorithmic bias, decision traceability and system validation cannot be treated as secondary considerations. Building trust requires more than technical performance. It demands clear accountability, robust validation and continuous oversight throughout the lifecycle of AI-enabled systems. Manufacturers that address these requirements early will be better positioned to meet regulatory expectations and build long-term confidence among regulators, customers, clinicians and patients.

STANDARDS AND GLOBAL ACCESS

International standards, such as ISO frameworks, continue to define the benchmark for safety, quality and compliance. However, consistent execution requires more than meeting formal requirements. Good Manufacturing Practice (GMP) must be maintained across the entire production and supplier ecosystem.

Automation helps translate these standards into reproducible processes. By relying on validated methods, standardised equipment and documented process parameters, manufacturers can achieve consistent quality outcomes across different production environments. This becomes particularly important when manufacturing networks expand across multiple sites or regions.

Recent global disruptions have also shown the limits of highly centralised production. Relying on a single site can reduce responsiveness and increase supply risk. Establishing automated manufacturing closer to end markets can therefore strengthen resilience, improve flexibility and support more stable supply chains. To make this possible, production systems must be replicable, scalable and capable of delivering the same quality standards across locations.

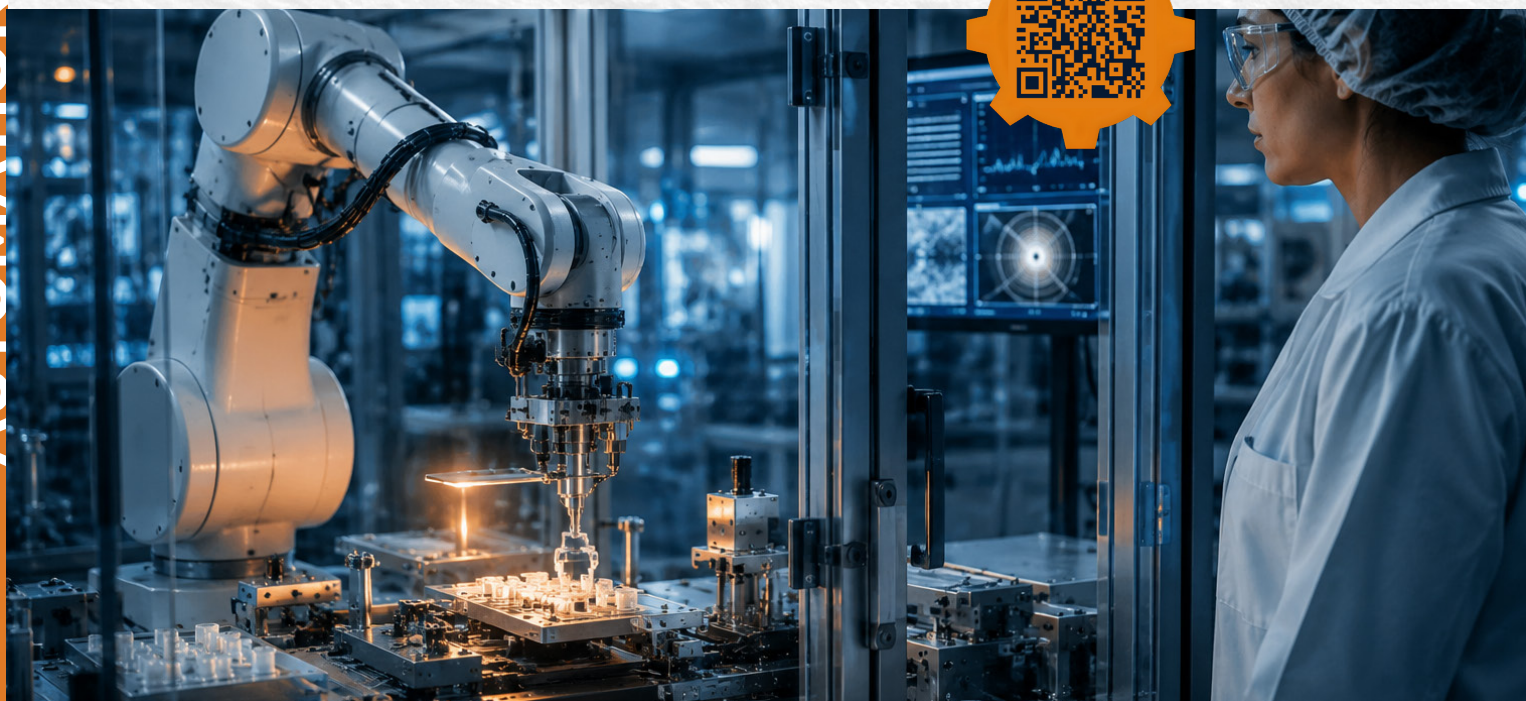
In this context, automation is not only a production technology. It becomes a foundation for global access, helping manufacturers bring critical products to market more reliably and closer to the people who need them.

A HUMAN-CENTERED FUTURE FOR MANUFACTURING

The future of manufacturing will not be defined by technology alone. It will depend on how effectively companies align innovation with safety, usability and human needs. AI, robotics and automation offer significant potential to accelerate development, improve quality and support more personalised forms of care. Their value, however, depends on responsible implementation.

Manufacturers that embed these capabilities into every stage of development will be better equipped to meet regulatory expectations and build long-term trust. This trust matters not only to authorities and customers but also to clinicians and patients who rely on the safety and performance of the final product.

The next era of manufacturing will therefore be shaped by companies that can combine speed with responsibility. Those that succeed will not simply automate existing processes. They will build production environments that make innovation scalable, compliant and trustworthy from the start.

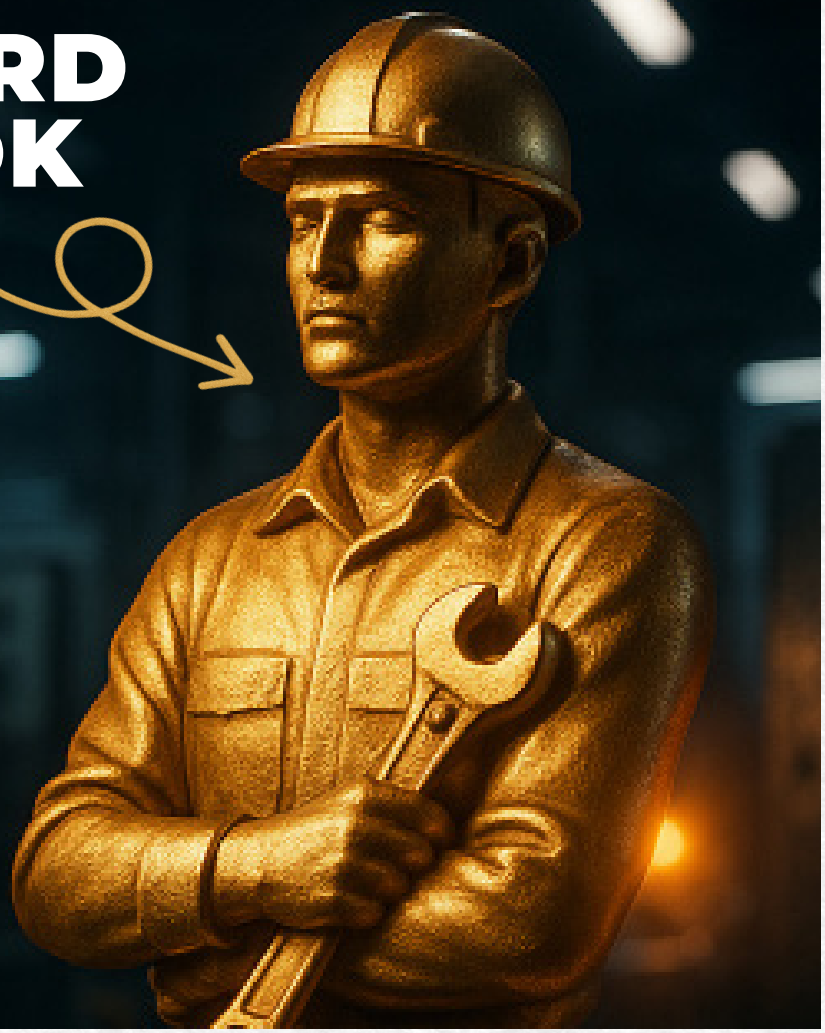


YOUR AWARD WON'T LOOK LIKE THIS

But it will inspire the same attention.

The Industrial Innovation Awards are coming.

Sign up to receive award updates:



DataCentral

Get beyond the rack.

The new site for news and analysis of the business and engineering of data centres.

From cloud to concrete and server racks to building systems, we cover every square foot of the data centre sector — and bring you the latest.

→ **Scan to visit DataCentral.**



https://data-central.co.uk/



FROM SKILLS SHORTAGE TO SKILLS EVOLUTION

Mark Gray, UK Sales Manager for Teradyne Robotics, explores how advanced automation and collaborative robots are enabling businesses to grow while helping employees build new skills, work more efficiently and take on higher-value roles.



The global industrial sector is at a crossroads. Amid ongoing disruption from geopolitical uncertainty, inflation, aging workforces and fragile supply chains, business leaders are rethinking how work is delivered.

Automation is moving up the agenda, but perceptions remain somewhat mixed. Rather than simply replacing workers, it is more often reshaping and supporting how work is done.

The latest generation of collaborative industrial robots (cobots) is reshaping how people and machines work together. Rather than replacing workers, robots take on repetitive, physically demanding tasks, allowing employees to focus on higher-value work that requires judgment and expertise.

To stay competitive, the industry must embrace this shift and rethink how people and automation work together.

THE SKILLS GAP AS A BARRIER TO GROWTH

The manufacturing industry is facing a growing skills gap driven by an ageing workforce and rapid technological advancements. Workers also want safer, more flexible workloads which means that manual, repetitive roles remain the hardest to fill.

It's, therefore, no surprise that there's an estimated 2.4 million jobs due to be left unfilled between 2018 and 2028.

What this means in manufacturing is more bottlenecks, slower growth and increased costs as businesses struggle to scale operations and compete more effectively.

TECHNOLOGY THAT SUPPORTS, NOT REPLACES

Where repetitive roles remain hard to recruit and skilled operatives used on routine tasks, businesses can see growth restricted.

Cobots – collaborative industrial robots designed to be able to work safely alongside people – are emerging as a practical and scalable answer to global labour shortages, especially in roles that are physically demanding, repetitive, or difficult to staff.

An overwhelming 91% of respondents in our State of Industrial Automation 2025 survey believe cobots could help reduce global labour shortages by at least 10%.

Cobots are designed to work alongside existing systems, taking on complex or awkward tasks that are hard to automate. Their flexibility allows businesses to introduce automation gradually, in ways that support and adapt to the current workforce.

Universal Robots and Mobile Industrial Robots (MiR) cobots and autonomous mobile robots (AMRs – robots that navigate independently to transport materials) are designed to support a range of manufacturing tasks.

Whether that's repetitive assembly and precision handling to internal logistics and material transport, they help enhance efficiency and productivity by allowing employees to focus on the higher-value and more engaging tasks at work.

And when businesses grow and look to automation and new technologies, they continue to need more people, not fewer – often creating new opportunities in higher-skilled, higher-value roles across operations, engineering, customer support and technical services.

This is backed up by research by the Copenhagen Business School as Danish companies that adopt industrial robots tend to grow rather than shrink. They become larger, more productive, and often employ more people.

IT'S POSSIBLE NOW

More than half of UK businesses in our State of Industrial Automation 2025 survey identified robotics and automation as the most transformative technologies by 2030, with 73% citing productivity as the primary driver. Real-world deployments are already proving why.

At Fu Zhuan Steel, for example, a UR12e cobot is used to automate laser welding in high-mix, low-volume production, reducing training time from over a month to just a day and enabling more employees to operate advanced automation.

At Volvo, robots improve employee wellbeing by removing dull, repetitive and physically demanding tasks. This reduces injuries and sick leave, while enabling safer, more meaningful roles that support skill development, job satisfaction, and a more inclusive, attractive workplace.



There are also clear gains in intralogistics. At VIBO's Trissino plant, the MiR1200 Pallet Jack handles full pallet transport cycles autonomously, improving efficiency and working conditions.

The impact is clear: automation improves productivity while freeing employees from repetitive tasks. By taking on physically demanding work, cobots reduce strain and injury risk, supporting staff wellbeing.

This enables employees to focus on higher-value activities in a safer, more sustainable working environment, enhancing both performance and job satisfaction. It also supports improved job quality and helps create more sustainable, long-term employment opportunities.

RETHINK THE FUTURE OF AUTOMATION

The future of manufacturing will be shaped by collaboration between people and automation, not a choice between the two. Businesses can start small by automating a single role or intralogistics at first, before scaling more strategically over time.

As this transition accelerates, collaborative robots will play a key role in enabling organisations to adopt flexible, accessible automation that supports both growth and workforce development, while helping businesses evolve skills, improve job quality, and build a more resilient workforce for the future.

The future of manufacturing will not be defined by fewer people, but as has always been the way, by how effectively technology empowers them to do more and scale up.



IS IT TIME FOR FOOD INNOVATION TO CATCH UP TO GLP-1S?

*By Greg Holgate, Business Development Manager (Pharma), **ACI Group***

Until recently, food brands and manufacturers targeting consumers focused on weight loss and weight management were primarily concerned with reducing overall calorie intake while still delivering strong organoleptic and sensory performance. This was typically achieved through formulations designed to increase satiety by boosting protein and fibre content and reducing sugar, fat and overall energy density..

The result has been a steady rise in high-protein yoghurts, reduced-sugar beverages, fortified snack bars, meal replacements and portion-controlled convenience foods. Yet many traditional 'diet' products still struggle to deliver genuine sensory satisfaction, often characterised by thin textures, limited indulgence and short-lived fullness. As a result, consumers can remain vulnerable to rebound snacking and poor long-term adherence to calorie-restricted eating plans.

However, the rapid rise of GLP-1 therapies is forcing a much deeper rethink of how consumers experience hunger while in treatment, and how they manage appetite once treatment ends.

GLP-1 medications do far more than suppress appetite. These medications can fundamentally interrupt long-established eating behaviours, reward responses and internal hunger cues. For many consumers, foods they once craved suddenly become unappealing, portion sizes shrink dramatically and eating itself becomes less emotionally rewarding.

Read this, and more of the latest developments in food processing and packaging, online on **IN Food**

in-food.co.uk/

This creates an entirely new challenge for food manufacturers: how do you develop products for consumers who may physically want to eat less, but still need nutrient-dense foods that deliver satisfaction, nourishment, pleasure and long-term eating confidence? The opportunity is no longer simply about helping consumers eat less, but about helping them rebuild a sustainable relationship with eating itself.

SMALLER, NUTRIENT-DENSE PORTIONS

One of the biggest behavioural shifts emerging from GLP-1 use is a growing preference for smaller meal volumes. Consumers often report struggling with large portions, rich meals, heavy textures or highly indulgent products during treatment. This creates demand for food products that are not only available in smaller, nutrient-dense portions but are sensory satisfying, metabolically balanced and easy to digest.

Consumers using GLP-1 therapies frequently consume substantially fewer calories overall, which can unintentionally reduce intake of essential nutrients.

This may contribute to fatigue and side effects, including sarcopenia (muscle loss) and hair thinning. Common nutritional concerns during GLP-1 use include inadequate protein intake, low fibre consumption, dehydration, reduced micronutrient intake and insufficient calories to preserve lean body mass during weight loss.

Protein, including hybrid proteins, becomes particularly important as rapid weight loss can increase the risk of muscle loss alongside fat reduction. Many healthcare professionals now encourage higher protein intake to help preserve muscle mass, physical function and metabolic health. In addition to nutritional gaps, many consumers also struggle with nausea, satiety, digestive discomfort, and food aversions.

This is creating significant opportunities for high-protein mini-meals, nutrient-dense smoothies and fibre-fortified dairy and snack formats that are easy to digest while still delivering complete nutritional and meaningful satisfaction.

Retailers and brands are already beginning to move in this direction. Marks & Spencer, for example, has developed smaller format meal concepts high in protein and fibre that align with consumer needs. However, the category is still largely underdeveloped specifically for GLP-1 consumers.

WHAT HAPPENS WHEN APPETITE RETURNS?

One of the most important, and least discussed, implications of GLP-1 therapies is that appetite suppression is not permanent. With millions of consumers going off these medications when their goal weight is reached, a new challenge is emerging around what to do when hunger signals and food noise return.

This can be a surprisingly complex adjustment. Consumers may experience hunger cues that feel unfamiliar, find that their satiety thresholds have shifted, and develop anxiety about overeating and regaining weight. Some will struggle to judge appropriate portions, while others will find it difficult to distinguish between physical hunger and emotional appetite. For many, the challenge is no longer weight loss itself but learning how to trust their appetite again.

This creates significant risk for rebound overeating, binge episodes, blood sugar instability and emotional eating cycles once treatment stops or dosage changes. Managing when to eat, how much to eat, and how to interpret hunger cues may become one of the next major frontiers in food science and product innovation.

STRUCTURED SATISFACTION

Traditionally, many health-focused products have been designed around restriction: fewer calories, less fat, lower sugar. But post-GLP-1 consumers are not necessarily looking for restriction in the longer term. What they are seeking is reassurance that the food they choose to eat can still feel indulgent without triggering loss of control. In essence, they are looking for eating to feel manageable again.

This is particularly important because many modern processed foods are optimised for maximum palatability and repeat consumption behaviour. Highly refined combinations of sugar, fat, salt, fast-digesting carbohydrates, and flavour enhancers can overstimulate reward pathways, encourage rapid eating, and weaken natural satiety responses.



Texture also plays a role. Soft, low-chew foods that dissolve quickly or deliver intense flavour release can reduce sensory fatigue and make it easier to overconsume before fullness signals register.

Many ultra-processed products are formulated around what food scientists call the 'bliss point' – the precise balance of sugar, fat, salt, and flavour intensity that maximises pleasure and encourages continued eating behaviour. Large portion formats, hyper-palatable coatings, layered crunch textures, rapid melt characteristics, and high glycaemic carbohydrate systems can all contribute to reduced portion awareness and rebound hunger shortly after eating.

For consumers emerging from GLP-1 therapies, this creates a potential vulnerability. As appetite and reward responses recalibrate, foods designed primarily for overconsumption may feel increasingly difficult to self-regulate around, particularly for individuals rebuilding confidence in hunger cues and portion control.

This creates an opportunity for manufacturers to rethink indulgence itself. The next generation of products may need to deliver satisfaction without hyper-stimulation. That means combining pleasure, satiety, nutrient density, slower energy release, and sensory completeness in ways that support appetite stability rather than override it.

This brings us to the idea of 'structured satisfaction' – the ability of a food product to deliver fullness, pleasure and sensory satisfaction in portions that are manageable without encouraging overconsumption. Importantly, this goes beyond simple satiety. It combines physiological response in the gut with the behavioural and emotional experience of eating. A product might meet all the right nutritional targets on paper, but if it leaves consumers psychologically unsatisfied or prone to rebound hunger, it fails the real-world test of sustainable eating behaviour.

PREVENTING SUGAR CRASHES & REBOUND HUNGER

As consumers transition away from active appetite suppression, one of the biggest nutritional risks may not simply be weight regain, but a return to appetite dysregulation.

Consumers who have become accustomed to reduced appetite may unintentionally under-eat earlier in the day only to experience intense cravings later, particularly for high-rewarding sugar and fat-rich foods. Rapid blood glucose swings can further amplify fatigue, cravings and overeating behaviours.

This signals a need for products specifically formulated to support appetite stability and glycaemic balance. Foods that combine protein, fibre, healthy fats and slower-digesting carbohydrates may help to moderate post-meal glucose spikes and reduce rapid hunger rebounds.

This is moving food formulation beyond simple calorie reduction and towards designing products that support sustained energy release, steadier appetite patterns and longer-lasting satisfaction.



INGREDIENT SYSTEMS THAT SUPPORT EATING BEHAVIOUR

At ACI Group, we see growing demand for ingredient systems that help developers formulate products not just for nutrient targets, but for the eating experience itself.

Hybrid proteins remain a validated tool for satiety support without heaviness, sensory fatigue or excessive portion burden. Similarly, fibre innovation is entering a new phase. Functional fibres can support appetite pacing, glycaemic stability and digestive comfort – important for consumers recalibrating their hunger cues.

Texture is also important post-GLP-1. Emerging research continues to show that oral processing, chew rate, viscosity and texture complexity all influence satiation and eating behaviour. Foods designed with layered textures, balanced flavour intensity and more engaging mouthfeel, may help consumers to experience greater satisfaction from smaller portions without feeling deprived.

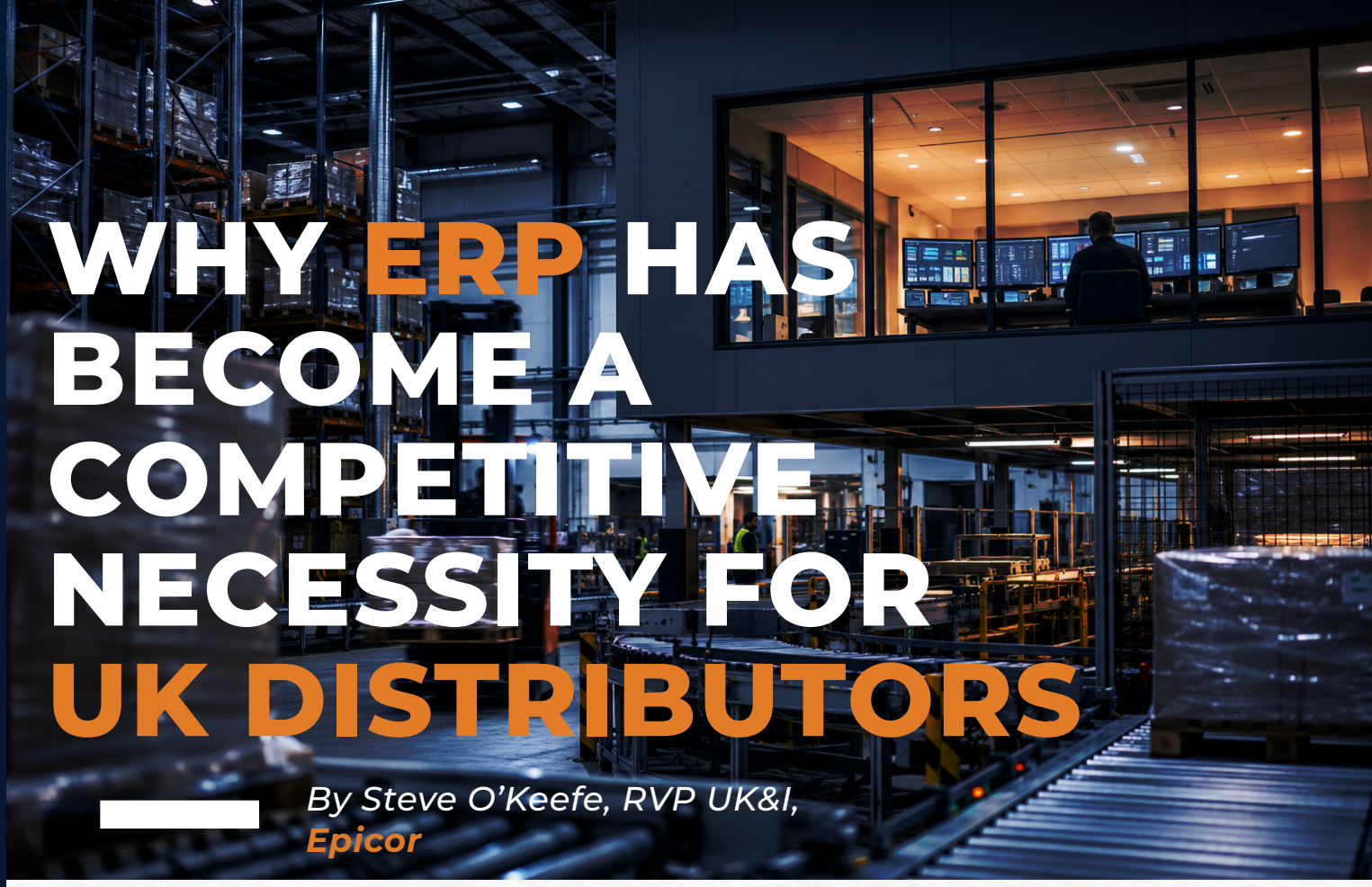
A DEFINING MOMENT FOR FOOD INNOVATION

The scale of GLP-1 adoption means this is no longer a niche wellness trend. It represents a massive shift in consumer eating behaviour that could influence food expectations across categories for years to come.

The brands that succeed in this new environment will be those that understand that consumers do not want to feel restricted forever. They want to feel capable of eating well again. For ingredient partners, this creates an opportunity to become far more than raw material suppliers. It creates an opportunity to help manufacturers design the next generation of food products around appetite resilience, behavioural nutrition and long-term eating confidence.

At ACI Group, we believe the future of food innovation lies not in suppressing appetite further, but in helping consumers rebuild a healthier, more sustainable relationship with it.





WHY ERP HAS BECOME A COMPETITIVE NECESSITY FOR UK DISTRIBUTORS

By Steve O'Keefe, RVP UK&I,
Epicor

They say that a week is a long time in politics. It's also a long time in business. Just about everyone I've spoken to is struggling to keep up with events. It's not just the pace of change that's a problem. It's the fact that every time one issue settles down, something else immediately takes its place.

It's a topic discussed at length in an IDC report published in March 2026, which spelt out exactly what the sector is up against.

It found that almost three-quarters (73%) of distribution companies think that a recession is likely in the next year, with six in ten (60%) admitting that they were affected by higher prices and increased costs.

Volatility is no longer something that happens once in a while. It's now the norm. And the problem is compounded because too few companies have modern ERP systems to help them manage operational ups and downs.

HOW THE LACK OF REAL-TIME VISIBILITY IS SLOWING RESPONSE TO SUPPLY CHAIN SHOCKS

In part, it's because too many businesses are hanging on to their legacy ERP systems and manual processes. But this approach is only putting off the inevitable. Why? Because distribution is now a real-time industry.

Prices move faster. Supply chains shift more quickly. Customer expectations are higher. Sustainability reporting requirements are growing. And if you follow the news as I do, you'll know that disruption can appear from almost anywhere with very little warning.

Legacy ERP cannot cope with the modern world. Worse, it acts as a pinchpoint that fails to provide full visibility and costs more to operate.

"The world has moved on when it comes to data and transparency," said one unnamed CEO who took part in the report. "You can't manage it on a spreadsheet or a legacy application anymore.

"You need a single data truth. Whether it's ease of access for employees, visibility for customers, traceability from suppliers, or regulatory compliance, access to dynamic and real-time data is non-negotiable," they said.

And that single source of trust is essential when supply chains are experiencing the kinds of shocks that are increasingly becoming an everyday occurrence.

"Without ERP modernisation, organisations in the U.K. and Ireland essentially stall their business," the report warned. "They cannot access the insights needed to compete in today's market, lack the critical tools and technologies for employees, forgo important optimisation improvements, and miss opportunities to reduce costs and strengthen resilience and security."

WHY LEGACY ERP SYSTEMS ARE NOW A LIABILITY, NOT A SAFETY NET

But what happens when firms do invest in modern ERP? One of the report's contributors, Steve Standley, Operations Manager at BES, explained how they were able to integrate their new ERP with their warehouse operations, website, and finance systems.

"That means our employees have the data they need to process orders more accurately and quickly, our customers have all the data they need at their fingertips, and accounting sees everything as it happens. So, modernising our ERP has helped bring out new capabilities in other systems and processes, and helps us grow at the pace we want," said Steve.

But there's also another side worth exploring. Those distributors that invest in modern ERP are gaining significant competitive advantage over those that don't.

In effect, what we're seeing is the emergence of a two-speed sector where modern ERP delivers real-time visibility and the agility to operate during turbulent times, while those holding on to legacy systems – in effect, those in the slow lane – will increasingly be at a competitive disadvantage.

As one unnamed CIO told IDC: "Not modernising your ERP system and relying on an on-premises legacy product is a going out of business strategy. It's as simple as that. You either modernise, or you don't survive."

The important takeaway, though, is that ERP isn't simply about investing in technology. Neither is it about mirroring existing systems and switching out old tech for new.

Instead, it's about fundamentally changing the way you operate.

In other words, the goal is not simply to modernise systems but to build a business that is better equipped to handle uncertainty.

After all, it's always difficult to predict what's going to happen in the future. By the time you read this, who knows what new event is keeping business leaders awake at night? Another geopolitical shock? Another spike in energy prices? Another supply chain disruption? And that's the point.

None of us knows what's coming down the line, so distribution businesses can no longer afford to operate as though instability is temporary or that things will eventually settle back down again. If businesses want to stay ahead of events – rather than be dictated by them – then they need the systems and processes in place to provide real-time visibility. And in doing so, they will be able to respond faster, make better decisions and build the resilience needed to thrive in uncertain times.

UPGRADING LEGACY PLATFORMS FOR NEXT GENERATION CONNECTIVITY

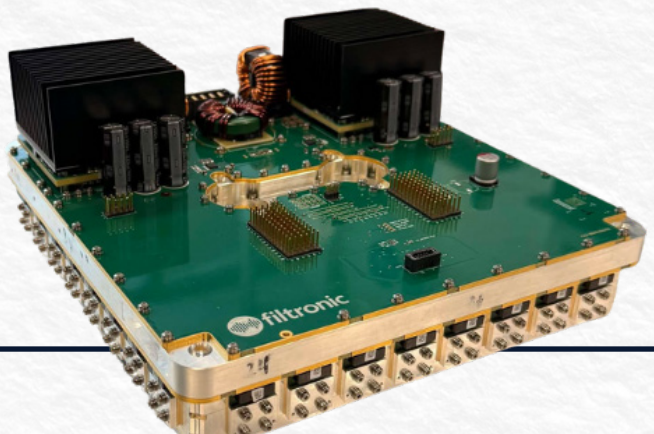
By Ashley Dove, Senior Advisor, Filtronic

The future of connectivity is no longer being built on standalone systems. Instead, we are becoming increasingly reliant on a hybrid and tightly integrated ecosystem of terrestrial and non-terrestrial networks. Depending on the use case fibre, cellular, satellite and airborne platforms can all play their part in meeting coverage, capacity, resilience and latency requirements.

For critical communications, whether in defence, aerospace or emergency response, this hybrid approach is becoming essential. Terrestrial infrastructure provides high-capacity, low-latency connectivity in dense environments, but it is inherently limited by geography and vulnerability to disruption. Non-terrestrial networks (NTNs), particularly low-earth orbit (LEO) constellations, extend coverage globally and add resilience, but introduce their own challenges in scale, power, and complexity. The real opportunity lies in how effectively these layers can operate together, dynamically sharing load and maintaining service continuity under any conditions.

This convergence is redefining expectations at the network level. Systems must now support seamless handover between ground and space, adapt in real time to changing demand, and deliver consistent performance across highly diverse operating environments. Achieving this depends not only on advances in software and network orchestration, but also on fundamental improvements in the RF layer—where signal generation, amplification, and transmission ultimately determine what is possible.

In this context, approaches that enable tighter integration between RF performance and digital control are becoming increasingly important. Architectures that allow greater flexibility in how signals are generated, combined, and distributed—while maintaining efficiency and reliability at high frequencies—are key enablers of a future hybrid network operation. This kind of capability underpins the practical realisation of distributed, software-defined infrastructures that can scale across both terrestrial and non-terrestrial domains.



THE LIMITS OF LEGACY RF ARCHITECTURES

For many operators, there's a lot at stake. Their current systems represent years of investment and proven performance. These platforms are trusted, resilient and deeply embedded in critical infrastructure. But they weren't built for the scale and complexity of today's data demands. That means the goal isn't to replace them outright, but to evolve them, extending their lifespan while boosting performance. And that process starts at the RF layer, where the fundamental limits of hardware shape what's possible.

Travelling Wave Tube Amplifiers (TWTAs) have long been a cornerstone of this layer. They've played a crucial role in delivering high-power transmission in satellite communications and have a well-earned reputation for reliability in tough conditions. But past success doesn't automatically make them fit for the future.

As the industry pushes into higher frequencies, broader bandwidths, and more flexible network designs, the limitations of TWTA-based systems are becoming harder to ignore. One of the biggest challenges is how they are measured, for TWTAs the saturated power output (Psat) is often seen as a key performance specification, but amplifiers will never actually operate at this maximum power level in satellite communications systems. What really matters is the linear power output (Plin) – the usable, distortion-free output power of the amplifier, which is where SSPAs significantly outperform TWTAs. As systems scale up, power becomes a critical constraint. On top of that, maintenance requirements and lifecycle management can introduce delays and complexity in systems that increasingly need to be always-on and responsive. Perhaps most importantly, they lack built-in redundancy, which creates a risk in environments where resilience is no longer optional, it's expected.



MOVING UP THE SPECTRUM

These pressures are only increasing as communications move further up the frequency spectrum. While Ku-band has been a mainstay for years, Ka-band and even higher frequencies are now taking centre stage. Frequencies like Q/V-band and E-band are unlocking massive increases in data throughput, supporting everything from feeder links to inter-satellite communications and secure, low-latency connections. But these gains come with tougher technical demands, higher power density, stricter thermal management, more complex system integration and increasing complexity of repeatable manufacturing at scale.

This is where solid-state technology comes into play. Solid State Power Amplifiers (SSPAs), particularly those based on gallium nitride (GaN), represent a significant shift in how high-power amplification is delivered.

What's especially important is that moving to SSPAs doesn't have to mean disruption. Modern designs can match the form factor of existing TWTAs, making them true drop-in replacements. That removes one of the biggest barriers to upgrading. Operators can improve capacity, efficiency and resilience without redesigning their entire systems. In practical terms, it allows for steady, proactive evolution rather than reactive replacement.

CETEC ERP

Your ERP should be a solution, not a problem

MRP
ERP
QMS
CRM
MES



FULLY INTEGRATED

All-in-one system to centralize your entire business on a single, web-based platform.

SIMPLIFIED COMPLIANCE

Out-of-the-box lot/serial traceability and native QMS functionality makes quality efficient and audit ready.

BUILT TO SCALE

Highly configurable manufacturing platform to handle increasing complexity as you grow.

Complete, versatile, and powerful

The Cetec ERP platform has everything you need to run all areas of your manufacturing business effectively. The high impact system includes powerful features and tools that you might expect only from higher cost providers, yet it is surprisingly affordable and simple to use.

Contact us to schedule a demo and get familiar with our BUILD YOUR WAY solutions.

BUILD YOUR WAY CETEC ERP

Scan QR or visit **cetecerp.com** to learn more

ENABLING RESILIENCE THROUGH ARCHITECTURE

The benefits of SSPAs aren't incremental, in fact they reshape system design. They tend to be more reliable because they eliminate vacuum-based components in favour of solid semiconductor technology. Redundancy can be built in, allowing systems to continue operating even if part of the amplifier chain fails. And because they're typically smaller and lighter, they're especially attractive in aerospace applications where space and weight matter.

But the real value of SSPAs goes beyond these advantages. They fit naturally with where communications systems are heading. Networks today are becoming software-defined and increasingly intelligent. Different orbital layers such as GEO, MEO and LEO are being integrated into unified architectures, while technologies like digital beamforming, AI-based optimisation, and software-defined radios are changing how spectrum is used.

In that kind of environment, hardware can't remain static. It needs to be part of the system's adaptability. SSPAs are well suited to this role, as they can integrate more easily with digital control systems and support faster, more flexible operation. This closer alignment between RF and digital layers is key to delivering the agility that next-generation networks require. It's not just about more bandwidth it's about enabling entirely new kinds of connectivity.

For engineers, moving from TWTA to SSPA presents both opportunities and responsibilities. While drop-in replacements make upgrades easier, they don't remove the need for careful system-level thinking. Factors like thermal performance, interface compatibility, and power distribution still need to be managed properly. At the same time, built-in redundancy opens the door to more resilient designs but only if it's thoughtfully integrated from the start.

FUTURE-PROOFING THE RF FOUNDATION

It's also important to look ahead. Decisions made now should reflect where systems are going, not just where they are today. Frequency planning, in particular, needs to account for future demand. As the industry continues pushing into higher bands, the ability to scale and adapt will be key to staying competitive.

Filtronic's work in high-frequency RF and millimetre-wave technology reflects this forward-looking mindset. Its development of GaN-based SSPAs for Ka, Q/V, and E-band applications shows a clear focus on enabling next-generation connectivity. These aren't just concepts, they're already being deployed in real systems, including high-capacity ground infrastructure for LEO constellations.

Just as importantly, there's a strong emphasis on practical implementation. By designing solutions that integrate with existing systems, Filtronic helps operators modernise without disruption. That balance between pushing technology forward and making it usable in real-world environments is crucial. Innovation only matters if it can be implemented smoothly and effectively.

Stepping back, the bigger picture is clear. The future of communications won't be defined solely by entirely new platforms, but by how well we can upgrade and evolve what's already in place. Legacy systems aren't a limitation, they're an opportunity, as long as they can be modernised in the right way. Solid-state amplifier technology provides a realistic and scalable path to make that happen.

Ultimately, upgrading the RF layer is a strategic move. It affects not just individual system performance, but how those systems connect into the wider, increasingly interconnected networks of the future. In a world where capacity, resilience, and adaptability are critical, the shift from TWTA to SSPA isn't just a technical improvement t's a necessary step toward keeping pace with next-generation communications.

INDUSTRIAL AI WON'T SCALE WITHOUT SOLID DATA FOUNDATIONS

*By Craig Gravina, CTO, **Semarchy***

97% of enterprises are investing in AI. 92% are confident they'll hit their goals. So why are more than half saying their biggest obstacle isn't cost or talent - it's data?.

Semarchy's 2026 State of MDM Report makes the gap plain: AI ambition is outpacing the foundations required to sustain it. Nowhere is that gap more costly than in industrial environments, where manufacturing runs on precision and trust. When data is fragmented or poorly governed, supply chains break down, decisions get made on bad information, and AI delivers the wrong answer faster.

WHY DATA FOUNDATIONS MATTER IN INDUSTRIAL SETTINGS

Manufacturing data challenges are amplified by the complexity of the work itself. Operations span vast ecosystems of suppliers, assets, production lines and logistics networks - each generating fragmented data in different formats.

Without a unified, well-governed data layer, this quickly leads to conflicting records: systems that can't agree on something as fundamental as a supplier name or a product specification. A mismatch at that level doesn't just create admin overhead. It can halt a production line.

This is why 66% of organisations now enforce data quality checks before AI consumption. Those that skip this step don't just risk poor model outputs - they risk compliance exposure, halted production, and financial losses that compound fast.

THE HIDDEN COST OF BUILDING AI ON POOR DATA

Rushing AI without fixing data foundations first creates what's increasingly being called "AI technical debt." These systems may deliver early wins, but they become expensive, fragile, and difficult to scale. With 35% of organisations still building AI without integrated data platforms, many are heading in that direction without realising it.

In manufacturing, this shows up as unreliable predictive maintenance, inconsistent supply chain insights, and AI that amplifies existing data problems rather than solving them. As regulatory scrutiny increases, so does the compliance risk - particularly as traceability becomes a baseline expectation, not a differentiator.



HOW MANUFACTURERS ARE BUILDING FOR SCALE

Data management needs to be treated as a core strategic function from the outset - not something retrofitted once AI starts to struggle.

Today, 65% of organisations use data management platforms to support AI, while half have implemented Master Data Management (MDM) to establish a single source of truth across critical domains. With MDM in place, teams across the business work from the same data: fewer errors, more reliable AI models, faster decisions.

A further 77% have integrated AI into their data governance frameworks, enabling outputs to be traced and decisions to be properly justified. That combination - unified data, governed AI - is what makes it possible to scale confidently beyond a pilot.

CLEAN DATA, REAL OUTCOMES

Clean data means teams are working from consistent, governed information across the organisation - not maintaining their own local versions and hoping they match.

One way this is achieved is through golden records: single, authoritative versions of key entities. When a predictive maintenance model flags a component for replacement, the golden record ensures the asset ID and all associated data are accurate and current. Teams act on a trusted foundation, not a best guess.

Data lineage matters equally. In practice, this means tagging data at the point of ingestion and tracking every transformation across systems — maintaining an auditable trail that teams can interrogate. As AI-driven decisions face greater scrutiny, that level of visibility stops being a nice-to-have and becomes a compliance requirement.

BUILD THE FOUNDATION BEFORE YOU SCALE

For industrial leaders, the path forward starts with the basics. Think big, start small.

Begin by auditing core data domains - products, suppliers, assets - to identify where inconsistencies live. Implement MDM to unify and standardise data across systems, creating a reliable foundation. Put governance and quality controls in place before scaling AI, not after encountering the consequences.

Platforms like Semarchy are designed exactly for this: consolidating MDM, data integration, and governance into a single environment, so manufacturers can move from data audit to production-ready AI in weeks, not years. Customers routinely go live in twelve weeks - with the data foundations to show for it.

The manufacturers that win the AI race won't be the ones who moved fastest. They'll be the ones who built right. Production-ready data isn't a prerequisite to tick off before AI begins - it's the infrastructure that determines whether AI ever delivers at scale.



PHYSICAL AI NEEDS A TRUSTED LAYER

By Marko Finnig,
VP, Head of Embedded Business Unit,
Tuxera

Physical AI is expected to unlock more than €430 billion in value across industries, powering autonomous systems in factories, vehicles, infrastructure, healthcare, logistics, and robotics. But unlike traditional cloud AI, these systems operate under real-world constraints that fundamentally change how AI infrastructure must behave. Physical AI platforms need a trusted data layer between sensors, models, storage, edge compute, updates, telemetry, validation, and lifecycle operations.

A large language model running in a cloud environment can tolerate occasional latency, dropped connections, or incomplete data without creating immediate operational consequences, but Physical AI systems cannot.

A robot operating on a factory floor cannot safely wait for a delayed cloud response before making a decision. Similarly, an autonomous industrial vehicle cannot behave unpredictably because sensor data arrived late under system load, and a machine recovering from a power interruption must resume operation predictably and reliably, not eventually.

As AI moves from digital environments into physical systems, the challenge shifts from scaling compute alone to ensuring systems behave reliably under real-world operating conditions. This is where the Physical AI data layer becomes critical. Models determine what the system can infer. The data layer determines whether it can keep behaving correctly and predictably in the real world across a long operational lifetime.

PHYSICAL AI CHANGES THE INFRASTRUCTURE PROBLEM

Much of today's AI conversation still focuses on models, accelerators, and compute performance. But in industrial environments, deployment challenges often emerge elsewhere.

Physical AI systems continuously generate operational data. Sensor streams, telemetry logs, software updates, configuration states, and machine outputs must all be captured, stored, recovered, and validated reliably in real time.

Unlike cloud-native environments, industrial AI systems frequently operate under constrained conditions. Connectivity may be intermittent, power interruptions are common, and many systems must continue operating autonomously at the edge for years using fixed hardware resources. Many Physical AI platforms are also optimised for compute performance rather than continuous data capture and recovery under sustained workloads.


IN THE KNOW
ON THE GO
Tune into the latest industrial views and insights with the Industrial News podcast.
Coming soon.
Guest booking now open.
Contact:
podcasts@industrialnews.co.uk

These constraints fundamentally change the role of infrastructure. In Physical AI systems, the data layer increasingly becomes part of system behaviour itself. If telemetry data becomes corrupted during a power interruption, engineers may lose the ability to reconstruct a safety event. If storage latency spikes under heavy workloads, sensor timing may shift enough to affect system decisions. If an interrupted update leaves system state inconsistent, autonomous machines may fail to recover predictably after restart.

Physical AI will not scale on model capability alone. It depends on a trusted data layer capable of capturing, moving, storing, recovering, replaying, and validating operational data consistently under real-world conditions. This matters for the entire Physical AI ecosystem. As platforms evolve across simulation, training, deployment, edge inference, telemetry, and continuous improvement, the data layer becomes the connective tissue between model development and real-world operation. Without trusted data capture, recovery, replay, and auditability, even highly capable models become difficult to validate, certify, and scale in production.

CONTROLLED ENVIRONMENTS HIDE REAL-WORLD PROBLEMS

Controlled demonstrations and pilot projects often hide the issues that emerge during long-term deployment.

Industrial systems may experience repeated brownouts, interrupted writes, fluctuating telemetry volumes, environmental stress, and changing workloads over many years of operation. At the same time, software-defined systems continue evolving through updates, diagnostics, and new AI-driven features.

Many failures also emerge gradually rather than catastrophically. Engineers may first encounter inconsistent recovery behaviour, corrupted telemetry logs, increasing latency under load, failed updates, or silent data corruption that remains difficult to detect during normal operation.

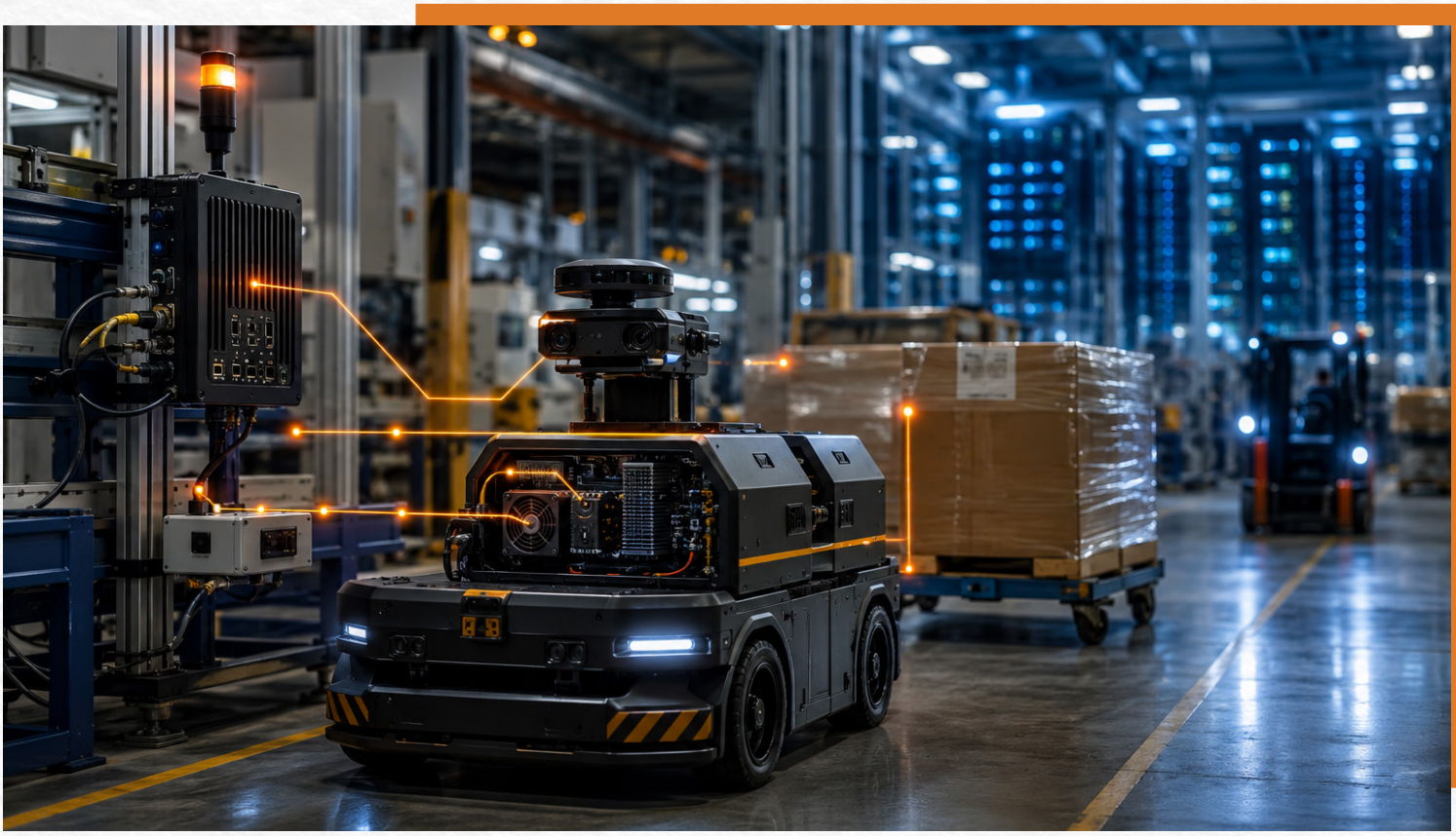
In some cases, two systems running identical models and control logic may still behave differently because of inconsistencies in sensor timing, cached state recovery, or storage latency under load. A delayed sensor frame arriving milliseconds late may alter how a system interprets its environment. Likewise, if an edge system experiences an ungraceful shutdown during a power outage, the way logs, cached data, and operational state are recovered can influence whether the system resumes predictably or behaves differently than expected.

These edge cases can become extremely difficult to reproduce during validation, certification, or incident investigation. If system behaviour cannot be reproduced consistently, scaling Physical AI deployment becomes significantly harder. In regulated industrial environments, incomplete operational logs or traceability gaps may also create compliance and auditability challenges.

THE POWER CHALLENGE

Power instability remains one of the most difficult realities in industrial and embedded system design. When power is interrupted during an active write operation, metadata updates may remain incomplete, files may only be partially written, telemetry logs can become corrupted, and the file system itself may enter an inconsistent state. In systems relying on over-the-air (OTA) updates, interruption may also leave software or firmware packages incomplete, preventing predictable and reliable restart behaviour.

In Physical AI systems, these failures have broader operational consequences because the affected data is often



mission-critical. Incomplete telemetry may prevent engineers from reconstructing a machine event, while corrupted state recovery may complicate root-cause analysis and delay validation across industrial fleets. This is why resilience in Physical AI environments increasingly depends on predictable and reliable recovery behaviour rather than simple uptime metrics alone.

FROM AI DEMONSTRATIONS TO REAL-WORLD DEPLOYMENT

Industrial Physical AI systems are highly write-intensive by nature. Robots, autonomous machines, and intelligent infrastructure continuously generate telemetry, diagnostics, event logs, and sensor data that often need to be buffered locally before synchronisation or long-term processing.

These workloads place sustained pressure on NAND flash storage over time. Continuous write-heavy activity can accelerate flash wear through write amplification, while garbage collection processes may introduce latency variability under load. As systems become increasingly software-defined, storage workloads may also evolve significantly years after deployment.

The next phase of Physical AI adoption will not be defined by model capability alone. As AI moves into machines, the differentiator will be whether organisations can build systems that remain predictable, auditable, and resilient under real-world operating conditions.

Physical AI platforms need a trusted data layer between sensors, models, storage, edge compute, updates, telemetry, validation, and lifecycle operations. The data layer can no longer be treated as passive infrastructure beneath the model. It is the foundation that allows Physical AI systems to capture what happened, recover safely, replay events, support validation, and earn trust over long operational lifecycles. As AI moves deeper into factories, infrastructure, transportation, and industrial automation, trusted data becomes foundational to real-world deployment at scale.

AI IS REDESIGNING INDUSTRIAL CONNECTIVITY. THE NETWORK MUST EVOLVE WITH IT.

By John Harrington,
Executive Vice-President & Head of Europe
Nokia

Every generation of communications infrastructure has been shaped by the workload it carries. While voice transformed one era, mobile broadband defined another. Today, AI is quickly becoming the defining workload of the network economy, bringing with it machine-to-machine interactions and autonomous systems that place entirely new demands on connectivity.

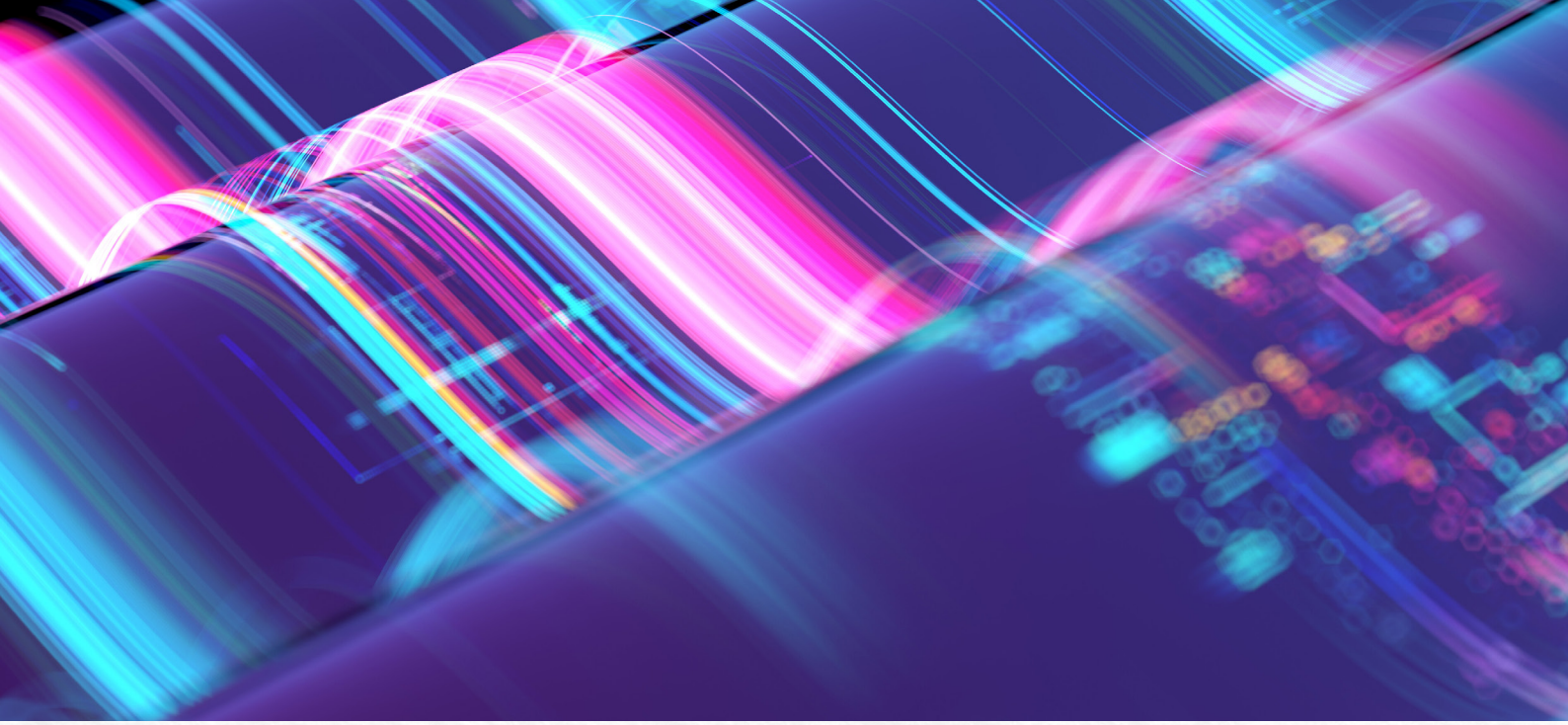
For industrial organisations, AI is already moving quickly into day-to-day operations. As decision-making increasingly shifts to software, sensors and machines, the network is no longer just a supporting layer; it is becoming a core enabler of performance. Manufacturing lines, logistics hubs, ports, utilities and transport networks are generating growing volumes of machine-to-machine traffic, real-time analytics and autonomous interactions. To support these workloads, the underlying network must deliver predictable performance, low latency and resilience at scale.

Until now many organisations have understandably focused their AI strategies on models, applications and data. But as AI moves deeper into operations, we need to look at how to ensure the infrastructure can keep pace.

AI DEMANDS A DIFFERENT FOUNDATION

Traditional enterprise networks were designed around human interactions: employees accessing applications, sharing data and communicating with one another. AI introduces a very different environment – one made up of continuous exchanges between machines, software and physical environments, creating patterns of traffic that are larger in scale and far less predictable.

Scaling networks may help, but it doesn't get to the heart of the problem. AI workloads make demands that conventional network infrastructure was never really built for, with deterministic performance being the critical element. In industrial settings where automated systems are making live calls on production, safety, and operational continuity, the data needs to arrive on time, every time, regardless of what else is happening on the network. Speed matters, but so does certainty.



This is what sets AI apart from earlier technology shifts: it places new demands not just on applications, but also on the infrastructure that supports them. Networks designed around older assumptions often need more than just an upgrade. This is where 6G comes into the frame. While much of the excitement around 6G focuses on faster connectivity, its greater significance may lie in the shift towards AI-native networks, where intelligence is embedded throughout the architecture. This enables machines to exchange data continuously and at scale, and across physical and digital environments that are becoming increasingly hard to separate.

Delivering on that promise will require coordinated evolution across radio access, core, IP, optical and cloud technologies, so the network can operate as one coordinated system. Treating each domain in isolation will make it harder to optimise how data, workloads and intelligence move across the system as a whole. As physical AI becomes more widespread, this level of coordination will only become more important.

EDGE COMPUTING STRENGTHENS THE WHOLE ARCHITECTURE

The point at which data is processed can be just as important as the point at which it is created, particularly when decisions need to be made in real time. Industrial organisations often need to analyse and act on information immediately, whether they are monitoring equipment, coordinating robotics or responding to changing conditions across a site. Processing these workloads closer to the source reduces delays and allows decisions to be made where they have the greatest operational value.

Digital twins, autonomous systems and other industrial AI applications depend on private wireless networks to connect assets; edge computing to process data with minimal delay and cloud infrastructure to coordinate information across locations. Bringing these elements together creates a stronger foundation for increasingly connected industrial environments.

In fact, many of the technologies already being adopted across industry are laying the groundwork for future innovation, where physical and digital environments become increasingly interconnected, and organisations can model, test and optimise operations before making changes in the real world. Digital twins already demonstrate the value of this approach, allowing manufacturers, utilities and transport operators to simulate assets or processes, explore different scenarios and identify potential issues before committing time and resources to physical implementation.

As these environments grow in scale and complexity, they increasingly depend on continuous streams of real-time data flowing between the physical infrastructure and its digital representation. This data can help organisations work more efficiently, reduce waste, develop new ideas and control physical systems remotely. However, to make this possible, networks will need to be fast, reliable and able to respond with very little delay. AI-native networks, edge computing and closer coordination across connectivity layers will help industrial environments become more intelligent, better connected and more responsive, providing the foundations for the industry of the future.

TRUST BECOMES PART OF NETWORK DESIGN

Security is fundamental, but AI brings wider questions of sovereignty, resilience, interoperability and long-term reliability. Organisations need to know where data is stored and processed, how systems behave under pressure, and whether different technologies can work together safely over time. Autonomous systems depend on information arriving securely, reliably and with very little delay.

These expectations place transparency, traceability and safety controls much closer to the heart of network architecture. Building them into the design from the beginning provides a stronger foundation than introducing them after deployment, particularly as organisations connect more systems across multiple domains. Cross-domain coordination and ecosystem collaboration also become increasingly important because trust cannot be achieved by any single technology operating in isolation.

PREPARING FOR THE NEXT PHASE OF INDUSTRIAL AI

Many industrial businesses are investing heavily in AI while relying on infrastructure designed for a different era. Taking a broader view of network strategy can help avoid creating bottlenecks that only become visible once autonomous systems begin operating at scale. Questions around architecture, interoperability and deterministic performance deserve the same attention as discussions about applications or data.

AI is becoming the defining workload of the network economy. Supporting it successfully will depend on infrastructure designed for autonomous interactions, trusted execution and coordinated operation across every layer of the network. The decisions organisations make about connectivity today will influence how effectively they can deploy, scale and trust AI for years to come.



PARTNER REPORTS | INDUSTRIAL NEWS

OWN THE CONVERSATION

The next Industrial News special report could be built around your market.

A sponsored article can open a conversation. A professionally produced report can give your brand a substantial campaign asset — developed around a live industry issue and built to keep working long after publication.

Our editorial team will help shape the brief, develop and write the report in a journalistic style, produce the finished design, host it as a gated download, and promote it across Industrial News channels.



EDITORIAL PLANNING • REPORT WRITING AND DESIGN • GATED LANDING PAGE • WEBSITE, NEWSLETTER, AND SOCIAL PROMOTION

PUT YOUR BRAND BEHIND THE NEXT INDUSTRY CONVERSATION.

Request examples and package options

jenn@industrialnews.co.uk

Explore partner report opportunities

HOW PLANNING REFORM COULD HELP SECURE THE UK'S INDUSTRIAL ENERGY

The government's proposal of sweeping planning reforms to allow single, small wind turbines on commercial sites to be built without the need for full planning consent shows a hugely positive shift for the UK.

That's according to David Woon, head of net zero engineering and operations at Ennovus Solutions. Here, he discusses how becoming more independent from the grid can strengthen our energy security, how this supports wider net zero targets and what else needs to be considered to allow projects to go ahead.

The recent announcements from the Department of Energy Security and Net Zero (DESNZ) signal a major shift from decades of regulatory requirements, representing much-needed progress amid a turbulent energy crisis.

Analysis by the Office for National Statistics found that output in energy-intensive industries, such as factories and farms, has fallen significantly since 2021 as these sectors continue to be squeezed financially by rising energy costs. However, by moving away from reliance on the grid and towards the ability to generate electricity independently could bring a suite of long-term benefits from both a financial, reliance and resilience perspective.

While the wind industry has been a longstanding pillar of the UK's net zero ambitions, the reality for the average factory owner, farmer, or school business manager has been a maze of red tape. Up until now, the permitted development (PD) route for wind has been largely confined to micro-scale turbines. At roughly 5kW, these are little more than domestic novelties, insufficient for the heavy lifting required by modern industry.

However, the government's new proposal for planning reforms highlights potential change. By allowing single, small wind turbines to be built on farms and commercial sites without the need for full planning consent, the government is finally acknowledging that decentralised energy is a matter of national economic resilience, not simply a green luxury.

THE SCALE OF OPPORTUNITY

The proposed reforms could fundamentally create mass energy independence for these key sectors. If approved, the changes to PD would allow for turbines capable of generating five times more annual electricity than the current scope. For commercially available turbines that sit within the new PD criteria, we are looking at a potential generation of around 100,000 kWh per year.

Unlike solar, which is a vital but intermittent contributor, wind provides a more constant generation source to tackle a business' needs. When we combine small-scale wind with roof-mounted PV and battery storage, we

have a strong triad of resilience. As well as boosting carbon efficiency, this could allow businesses to free their operational costs from the turbulent global energy market and regain more control.

While the reform is largely positive, a few key details require consideration, such as the proposed buffer zones. Engineering a wind project requires a deep understanding of site qualification and physical constraints, and so the government has also introduced some specific requirements around where these turbines can actually take shape.

The two proposed rules include the turbines being located at a distance from the land boundary no less than the tip height plus 10%, as well as being separated from any 'protected building' (homes, schools, etc) by ten times its rotor diameter.

To put that into perspective, a turbine with a 15m rotor diameter would require a 150m buffer from a neighbouring home. While these stipulations are understandable from a visual and noise impact perspective, they will naturally restrict many installations from occurring outside of rural areas or large-scale farmland.

However, there are already successful examples of wind turbines operating in public, semi-urban spaces under full planning permission. This includes Green Park turbine in Reading and the Kings Lynn hospital car park installation. These prove that wind can coexist with the built environment. As an industry, we would hope that these reforms mature and the buffer zones become more relaxed to allow schools and factories in more densely populated areas to participate in this energy revolution.

LOOKING BEYOND THE GRID

For these reforms to operate effectively, businesses must look beyond planning. High generation levels are not guaranteed – factors such as wind resource, limiting turbulent airflow from nearby tall obstructions (such as trees are buildings), foundation suitability, and, foundation suitability, and shadow flicker proximity to highways must be analysed thoroughly before works begin.

Despite these technical hurdles, the direction of travel is clear and the shift towards decentralised generation is the only way to strengthen the UK's energy security. By removing the expensive upfront surveys and planning hurdles, the government is providing a shortcut to grid independence.

In isolation, this proposal may not go far enough – but as part of the broader UK net zero strategy, it is a vital piece of the puzzle, empowering the private sector to take ownership of its carbon footprint and its cost base simultaneously.

At Ennovus Solutions, we see this as turning point. For the first time, the prospect of a farm, factory or school generating its own power through wind is a viable business strategy. The energy crisis has been a wake-up call, and these reforms are the first step in building a more resilient, independent and green industrial future.



FROM GREEN CLAIMS TO PROVEN PERFORMANCE

By Bin Lu, Executive Vice President, Power Products, ***Schneider Electric***

Industrial energy efficiency won't scale without stronger product-level environmental standards. Industrial organisations across Europe are grappling with a trilemma: tightening environmental regulation, rising expectations from customers, investors, and the public, and an era of high energy prices and intensifying competition. All of this is happening while they're still expected to deliver the same levels of performance, uptime, and reliability.

Yet a major barrier remains. For many categories of energy-intensive industrial equipment, the market still lacks consistent, comparable ways to validate environmental performance.

For the industrial sector to scale energy efficiency, it needs stronger, more widely adopted environmental standards for electrical products. The fastest way to do that is to expand the use of independent, science-based third-party certifications and harmonised product standards. This will enable buyers to compare products like-for-like, while manufacturers can be rewarded for real improvements.

THE CREDIBILITY GAP IN INDUSTRIAL SUSTAINABILITY CLAIMS

Regulations like the EU's Empowering Consumers for the Green Transition Directive — applying from September 2026 — will require companies to substantiate environmental claims with evidence or stop making them.

And yet, when it comes to environmental performance, the industry often relies on fragmented disclosures, self-reported claims, or sustainability statements that are hard to compare across suppliers.

This is where the market is vulnerable to greenwashing. According to the EU Commission, 53% of green claims give vague, misleading or unfounded information. This isn't because companies are deliberately being misleading, but because the system lacks a trusted yardstick. Ultimately this can lead to reputational damage and potential lawsuits.

THE THREE S'S: SAFETY, SUSTAINABILITY, SECURITY

Unlike consumer gadgets, industrial electrical equipment like circuit breakers, drives, switchgear components are designed to stay in service for decades. As a result, managers need to consider the long-term implications of what they install today, such as safety, reliability, and lifecycle sustainability.



In power distribution, safety has always been non-negotiable. Fire risk, electrical hazards, thermal performance, shocks, and failure modes aren't theoretical—they're real-world outcomes with serious consequences. That's why standards and certifications have historically focused heavily on safety. Most people only notice power products when something goes wrong: the power goes out, equipment fails, or an incident occurs.

But expectations are expanding. Customers and stakeholders increasingly want proof not only that products are safe, but that they are more sustainable, and, as systems become more connected, more secure. That means organisations need to validate and report on factors such as:

- Raw materials and where they're sourced
- Composition and restricted substances
- Manufacturing and environmental management criteria
- Packaging and logistics impacts
- Durability and design choices that extend useful life
- End-of-life pathways, including disassembly and recyclability

At the same time, as industrial operations become more automated, connected, and software-defined, cyber and information security are becoming part of the risk equation.

All of this is why industry needs a more complete picture through third-party certifications and standards.

SETTING A NEW BENCHMARK FOR SUSTAINABILITY IN INDUSTRIAL ELECTRICAL EQUIPMENT

Independent environmental labels have historically been more common in retail and consumer products; there's no reason the same shouldn't be true in industrial equipment.

As regulators and stakeholders demand more credible proof, product-level certification frameworks like ECOLOGO, now being applied to industrial electrical equipment can help the wider industry move from broad claims to comparable, independently verified data. At Schneider Electric, we recently became the first company to certify industrial equipment under UL's new UL 2711 standard — applied to our PowerPact molded case circuit breakers — precisely to prove the model works at industrial scale. This makes it easier for customers, partners, and policymakers to reward real improvements and scale more sustainable choices.

WHAT NEEDS TO HAPPEN NEXT

To truly unlock industrial energy efficiency at scale, we need to mainstream product-level environmental certification across more categories, align standards bodies and regulators around common definitions and metrics (rather than a patchwork of labels), and design for lifecycle outcomes now.

Industrial decarbonisation won't be delivered through promises alone. It will be won through measurable progress, proven performance, and transparency that earns trust.

FROM SCADA TO WEB-BASED CONTROL PLATFORMS

HOW INFRASTRUCTURE MANAGEMENT IS CHANGING

*By Max Fonner, CEO, **DITRA Solutions***

For many decades, SCADA systems were the standard solution for industrial and infrastructure control. They were usually designed as local systems for a specific facility, object or process.

In urban infrastructure, this created a fragmented model: street lighting, video surveillance, water systems, transformer substations and distribution cabinets could each have separate control systems. Each system worked on its own, but they were often isolated from one another.

Today, cities and infrastructure operators need connected systems that can exchange data, combine information and support better decision-making. Infrastructure can no longer operate only as separate technical islands.

THE TRADITIONAL UNDERSTANDING OF SCADA

Traditionally, SCADA is a supervisory control and data acquisition system used to monitor and control equipment. It communicates with field devices, controllers, sensors, meters and PLCs through industrial protocols such as Modbus, KNX, BACnet, OPC or similar standards.

A classic SCADA system is usually installed locally on a server or operator workstation. It provides screens, alarms, trends, equipment status and control buttons. This makes SCADA reliable and familiar, but also means it is often seen as a closed local system created for one specific task.

The main limitation appears when different systems need to work together. If several facilities or infrastructure systems use different SCADA platforms from different suppliers, connecting them into one environment can be complicated.

As a result, operators may have many systems that work individually, but no single operational picture. Data exists, but it is separated between different interfaces, databases and access rules.

NEW WEB ARCHITECTURE: WHY THE INDUSTRY IS MOVING IN THIS DIRECTION

The industry is increasingly moving toward web-based control platforms. The reason is not only a more modern browser interface, but a different architecture.

A modern web-based platform can provide monitoring, alarms, control commands, reports, dashboards and user access rights. At the same time, it can act as an integration layer between different systems.



Field devices still communicate through industrial protocols, but data is collected by gateways, controllers or concentrators and transferred to a server in a structured format. From there, it can be accessed through a web interface and exchanged with other platforms through OpenAPI, JSON and standard web services.

WHERE THE OLD MEETS THE NEW

SCADA and web-based platforms should not be compared simply as “old” and “new”. They have overlapping functions but different priorities.

SCADA is strong when the system boundaries are clear, the equipment is local and stable direct control is required and the ability to operate out of the box.

A web-based platform is better suited for distributed infrastructure. It adds integration, remote access, analytics, data exchange and interaction with other software systems. However, it usually requires more configuration work, especially for network settings and integrations.

A web-based platform does not automatically mean public cloud or open internet access. It can be deployed locally, inside the customer’s infrastructure, on a private server or in a hybrid architecture.

Security depends not on whether the interface is web-based or Windows-based, but on system design: user roles, access rights, encryption, audit logs, network segmentation, authentication and cybersecurity policies.

Traditional SCADA remains a strong solution where local control is the main requirement: a factory, pumping station, industrial building, production line or another clearly defined process. In such cases, SCADA can be practical, familiar and easier to deploy for a specific task.

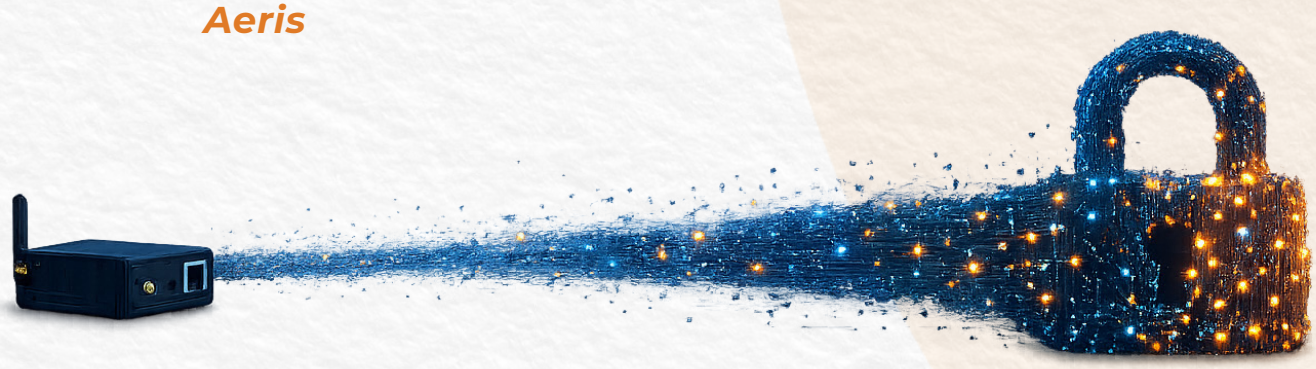
When the project involves multiple systems, distributed infrastructure and data exchange between platforms, web-based architecture becomes more suitable. This is especially important for urban infrastructure, where lighting, substations, utilities, transport and video systems need to work as part of a connected operational model.

The future is not about rejecting SCADA. It is about choosing the right architecture for each task. SCADA remains relevant for stable local control. A web-based platform with OpenAPI becomes the more logical direction when the project requires integration, scalability, analytics, remote access and data exchange.

SECURITY BY DESIGN

THE IMPORTANCE OF SECURING IOT AHEAD OF DEPLOYMENT

*By Syed Zaeem Hosain, Co-Founder and Chief Evangelist, **Aeris***



IoT security is no longer a challenge that can be addressed at deployment. It has become a design and lifecycle issue - one that must be integrated into devices from the start and maintained long after leaving the factory.

An evolving threat landscape is driving this shift. As cyberattacks adopt AI-driven techniques, attackers can identify and exploit vulnerabilities in firmware and embedded software at scale. A single weakness is no longer contained to one device - it can be replicated across industrial deployments, amplifying operational and financial risk.

The manufacturing sector is highly exposed. In industrial IoT and operational technology (OT) environments, connected devices are directly tied to physical processes, making cyber incidents a threat to production or equipment. High-profile incidents, including the disruption at Jaguar Land Rover (JLR), illustrate how compromising a single asset can trigger wider operational and economic consequences.

FROM ADD-ON SECURITY TO ENGINEERING REQUIREMENTS

Historically, IoT security has been treated as an extension of IT security, often addressed through patching, monitoring or network controls after deployment. That method is proving inadequate.

Regulatory frameworks, such as the Cyber Resilience Act (CRA) and NIS2, are placing greater accountability on manufacturers and solution providers. Organisations must demonstrate how devices are secured, updated and monitored throughout their lifecycle, making security a condition of compliance and market access. Vulnerabilities in firmware, provisioning and device identity are targeted more frequently, exposing gaps between device, network and application-layer protections.

The industry is increasingly adopting a 'security-by-design' approach, integrating protection into device architecture from the start. A vital aspect is hardware-rooted trust, using secure elements and trusted execution environments to establish device identity, secure boot processes and firmware integrity. This must be complemented by 'security-by-default' which ensures these protections are activated and monitored upon deployment rather than left inactive.

Secure provisioning is essential for authenticating and configuring devices before deployment, protecting credentials, keys, and identities from compromise. Weaknesses in this area can expose entire fleets to risks. Finally, 'security-by-demand' highlights the growing expectations from customers, regulators, and enterprise buyers for connected devices to have built-in security features. Procurement decisions increasingly prioritise evidence of secure development practices and compliance.

SECURING THE LIFECYCLE, NOT JUST THE DEVICE

Secure firmware updates are crucial. Updates need to be authenticated, verified, and delivered securely to prevent unauthorised modifications. This requires cryptographic signing, key management, and reliable delivery across distributed networks.

Security testing throughout the software development lifecycle (SDLC) is essential. Vulnerability scanning, penetration testing and validating third-party components, including open-source libraries, helps identify risks before deployment.

Supply chain transparency is becoming critical. Software Bills of Materials (SBOMs) offer a detailed inventory of the components within a device, allowing manufacturers to track dependencies and respond more effectively to any vulnerabilities. As regulatory requirements evolve, this level of visibility is essential for both compliance and operational resilience.

The most significant challenge remains achieving coordinated security across the entire IoT ecosystem. Industrial IoT deployments span multiple layers, including the device, the network and cloud-based applications. Securing them in isolation leaves gaps that attackers can exploit.

Many connected devices operate outside traditional enterprise boundaries, meaning threats may not be visible to standard IT security tools. At the same time, approaches designed for enterprise IT do not always translate effectively to embedded or OT environments.

Addressing this requires a more integrated approach. Security must be aligned across device behaviour, network activity and application-layer controls, supported by continuous monitoring and visibility across the IoT stack.

A NEW BASELINE FOR IOT SECURITY

Manufacturers and IoT solution providers must prioritise security as a core design principle rather than an afterthought. This means integrating hardware-based trust, secure provisioning, resilient updates and oversight throughout the lifecycle, alongside stronger ecosystem collaboration.

As IoT adoption accelerates, security is no longer just a compliance checkbox, it's the foundation of trust, resilience, and competitive advantage. Manufacturers and solution providers who embed protection from the first design decision to decommission will not only reduce risk, but also be best positioned to win in a more connected, regulated future.



IN CONVERSATION ROB DEMAIN, E2E-ASSURE

e2e-assure provides managed cyber defence and SOC services for organisations operating in high-risk, regulated, and increasingly connected environments. Its CUMULO platform sits at the centre of that service model, combining threat detection, analyst workflow, and AI-assisted investigation across IT and OT estates.

As AI moves from cyber-security promise into live operational decision-support, we speak with Rob Demain, CEO of e2e-assure, about what meaningful AI in the SOC should look like, why human oversight still matters, and how industrial organisations can defend systems where cyber risk now reaches into physical operations.

AI is now everywhere in cyber security. What does meaningful AI in the SOC actually look like?

"Meaningful AI isn't a chatbot bolted onto a Security Incident and Event Management (SIEM) solution. What matters is where you put the AI in the pipeline — and where you keep it out. Deterministic detection is an engineering problem. You solve it with stream-native infrastructure, not a language model. You don't want an LLM in the detection hot path because it's slow, non-deterministic and expensive at the volumes a Security Operations Centre (SOC) ingests.

"We keep the traditional SIEM as the system of truth and run the AI as a separate, parallel system alongside it, with hard boundaries. The AI reasons, enriches and judges. It never takes action. It informs the analyst or it informs the SIEM, and that is the safety layer.

"The UK government's GC3 pilot landed on the same architecture independently. It found the strongest results came from frontier models used as tightly scoped components inside a structured pipeline, broken into discrete task-specific harnesses to control false positives and hallucination. Scoped component, human in the loop, no autonomy. If a vendor's "AI SOC" can't tell you what the model is not allowed to do, that's your warning."



Where does CUMULO change the way analysts detect, assess, and respond to threats?

"Our CUMULO platform underpins our SOC and it reasons forward on the event stream instead of backwards from alerts. A traditional SOC waits for a rule to fire, then an analyst works backwards to reconstruct what happened. CUMULO reads every chapter, not just the last page. The deterministic engine funnels millions of events down to the handful worth judging. An AI reasoning layer sits alongside the SIEM, never inside it, assesses those candidates in context and hands its conclusions back to the analyst or the SIEM.

"The AI proposes. It never disposes. That gives you the speed of machine reasoning without the risk of letting a non-deterministic model pull a trigger on a live estate. The maturity arc is reactive, then proactive, then predictive, and predictive only earns the name if you saw the attack path before the attacker took it. The government pilot showed the upside of that reasoning even in a tightly scoped role: models traced vulnerabilities across service boundaries in a way traditional scanners can't, and linked business logic to technical detail. For the analyst it means less time stitching raw logs together and more time on the decision that actually needs a person."

How close can a modern SOC realistically get to detecting new threats as they emerge?

"Closer than the industry's track record suggests, but only if you're honest about what "new" means. You will not have a signature for a genuinely novel exploit. That's the Mythos-class problem. AI democratises zero-day production, so IOC and signature-based detection is structurally obsolete for anything new. What you can detect is behaviour and technique, because attackers still have to bypass a control, harvest credentials, move laterally and exfiltrate.

"The numbers set the pace you're racing against. CrowdStrike's 2026 Global Threat Report puts the average eCrime breakout time at 29 minutes and the fastest observed breakout at 27 seconds. Mandiant's M-Trends 2026 found the median time from initial access to handoff to a secondary threat group had collapsed to 22 seconds, down from more than eight hours in 2022. So "as they emerge" has to mean stream-native, behaviour-led detection measured in seconds, not a rule someone writes next week. The durable edge isn't a faster signature. It's knowing your own ground well enough to spot the technique the moment it touches your estate."

Why is human oversight still essential when AI is being used to accelerate security analysis?

"Because acceleration multiplies whatever you point it at, mistakes included. That's why our design never lets the AI take action. It informs the analyst or the SIEM and stops there. The human and the system of truth own every decision that moves anything.

"The government pilot is the clearest public evidence for keeping that boundary hard. Across nine departments, an agentic pipeline of triage, validator, auditor, tracer and judge stages still had a person check every line. The pipeline was agentic but the escalation was manual, with a team member re-verifying exposure and handling false positives. The teams concluded that agents generate candidate findings far faster than humans can validate them, and that it isn't how many issues you find but whether your triage points limited resource to where it matters.

"AI compresses the analysis. It doesn't carry accountability. When containment takes a customer offline, a person owns that call, not a model. The human is also where context lives: the maintenance window, the contractor finishing a migration, the "anomaly" that's actually business as usual."

ROB DEMAIN, CEO,
E2E-ASSURE

How do you stop AI from producing confident but unreliable conclusions in a live SOC environment?

"You don't let the model invent the facts. Keep the AI reasoning over deterministic evidence drawn from the system of truth, not free-associating from training data. It judges and explains what the detection layer found, with the underlying events cited back so a human can check the working.

"The government hackathons reached the same design by trial and error. The best teams ran deterministic scanners first to generate ranked leads, then layered model stages on top to compose findings into attack paths and confirm whether they were viable. Structure first, model second. Their headline lesson was that the model matters less than how it's used.

"With the right architecture, many near-frontier and frontier models perform comparably, and the best findings still lean heavily on human expertise. Constrain what the model is allowed to assert, make every conclusion traceable to source telemetry, and treat an unsourced claim as a defect, not a feature."

What does UK-sovereign cyber monitoring mean in practice, and why does it matter now?

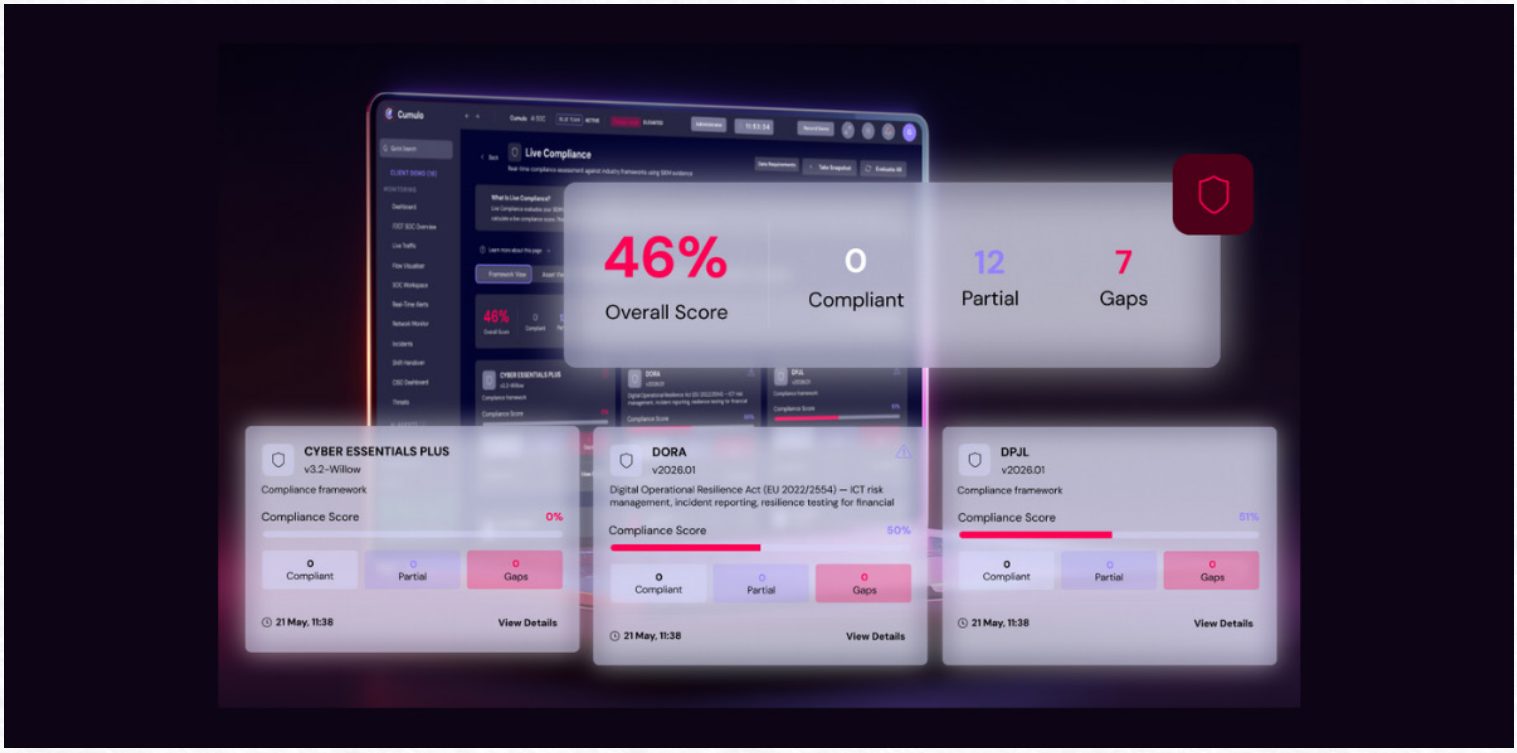
"This month made the case better than any pitch could. The US government pulled Anthropic's Fable 5 and Mythos 5 on 12 July. An export control directive barred access by any foreign national, including Anthropic's own employees, so the company disabled both models for every customer worldwide. A capability that customers had built around vanished in an evening, for reasons they didn't control. That's the headline.

"The lesson underneath it is dependency. If attackers have Mythos-class capability, defenders need it too, but relying on a frontier provider means relying on capability that can disappear overnight through a directive, an export order, a policy change or a terms-of-service update. The technique behind the recall reportedly works on other public models too, so this isn't one model, it's the direction of travel.

"UK-sovereign monitoring means the data, the detection and increasingly the AI models stay under UK jurisdiction and control. Local, on your own infrastructure, trained on your own ground. For regulated and CNI operators that's a resilience requirement, not a preference. And the durable edge was never raw model capability anyway. It's context. You know your estate, your identities, your normal, your compensating controls, your messy reality. An attacker's model doesn't. That doesn't get recalled."

Industrial organisations increasingly have connected IT and OT environments. What new and emerging risks does that create for security teams?

"Convergence collapses the air gap that used to be the OT world's main defence. Once IT and OT share connectivity, an IT-side compromise — phishing, a poisoned supply-chain package, a stolen credential — has a path to systems that move physical things, where the failure isn't a data breach but a safety or availability event. OT makes it harder still. The assets are long-lived, often unpatchable, and intolerant of the active scanning and agent deployment that IT security takes for granted. So teams inherit a bigger attack surface they can't defend with IT tooling, against attackers who understand the seam between the two better every year. The vectors we watch most closely — supply-chain compromise and edge and SOHO router footholds —land hardest at exactly that IT/OT boundary. The recurring failure is trusted legacy automation that everyone assumed was safe because it had always been there."



How can digital twin environments help organisations test cyber resilience without disrupting live operations?

"This is how you actually beat a Mythos-class attacker, and it works by inverting their advantage. The attacker's AI is powerful but blind. It doesn't know your estate, your identities, your processes, your compensating controls, your messy reality. So we build the AI that does.

"A digital twin, assembled from real observed telemetry, gives you a working model of the estate: identity, data flow, cloud and on-prem control paths, and how they connect. You exercise attacks against the twin rather than the live kit, which in OT is the difference between a useful test and an outage. You run synthetic telemetry through an isolated mirror of the detection engine to prove a detection fires before you ever depend on it in production. You can bias the traversal with named adversary profiles and ask: if this actor were in here, what path would they take, and would we see it?

"The defender's durable edge was never raw model capability. It's context. Their model learns code in the abstract. Ours learns your specific ground. That's how you win against Mythos. Not by matching its horsepower, but by knowing the terrain it's fighting on better than it ever can."

Compliance dashboards can easily become another reporting layer. How can they drive better security decisions?

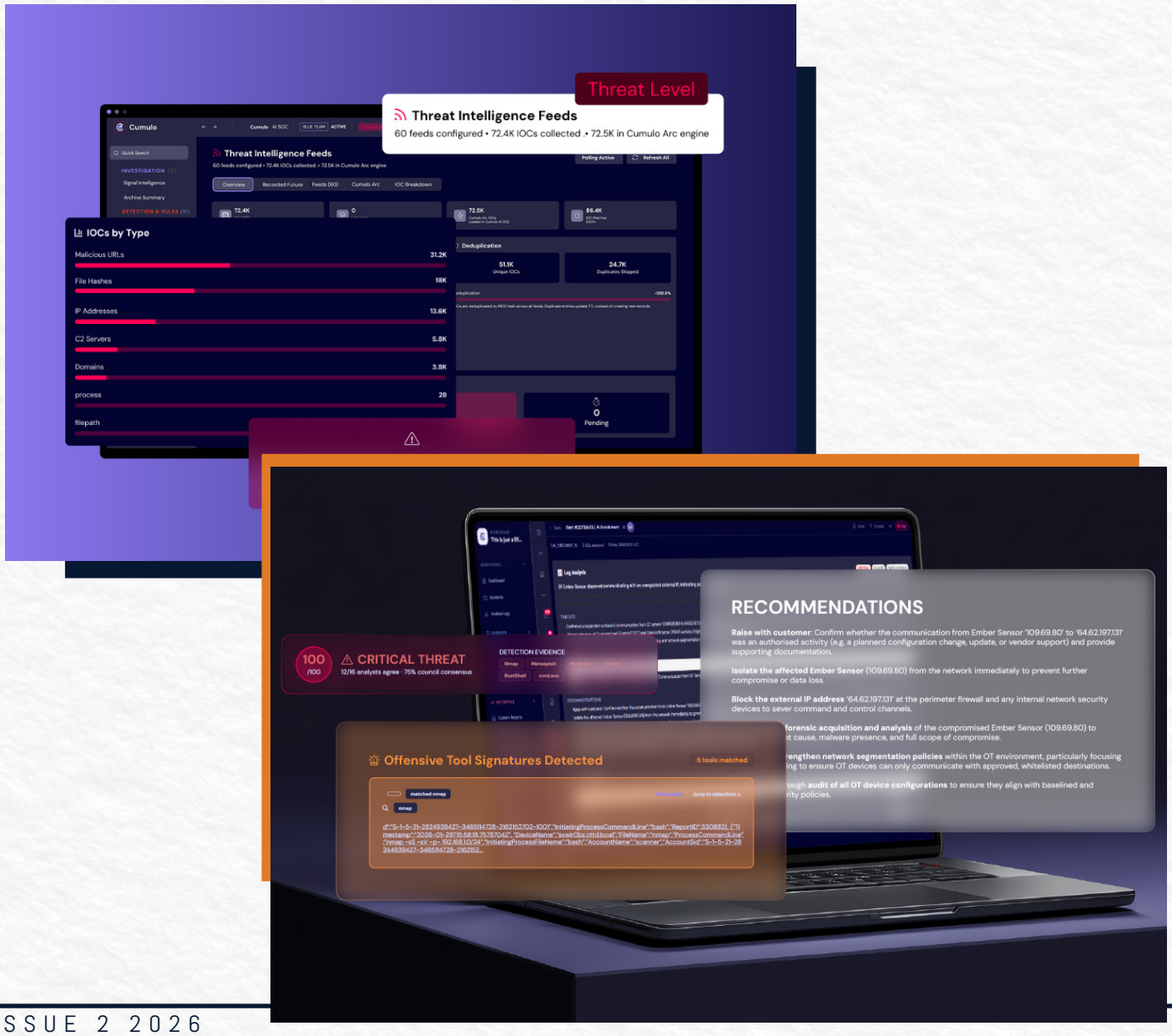
"A dashboard that only restates control status is overhead. To drive decisions it has to connect the framework — NCSC CAF, the incoming Cyber Security and Resilience Bill — to what your detection is actually doing, and be honest where the two diverge. The uncomfortable benchmark is CardinalOps' 2025 finding that organisations have detection coverage for roughly 21% of relevant techniques, with about 13% of rules broken outright.

"A dashboard earns its place when it surfaces that gap, green on the framework and dark on the coverage, and turns it into a prioritised engineering decision rather than a quarterly reassurance exercise. The government pilot makes the same point from the patching side. Finding isn't the same as fixing. Findings still have to enter the patch pipeline, and prioritisation, review and remediation all have to integrate without overwhelming the people doing the work. Compliance is the floor. The dashboard's job is to show the distance between the floor and your actual posture."

As AI takes on more of the triage and investigation workload, what should the future SOC analyst focus on?

"The work moves up the stack, not away. As AI absorbs the repetitive triage and first-pass investigation, the analyst's value shifts to judgement, adversary understanding and detection engineering: deciding what matters in context, hunting for the behaviour no rule has been written for yet, and turning what's learned into durable detection logic.

"The government pilot is a preview of the shape. Agents generated 407 findings across nine organisations for £13,000 in tokens, but the value came from humans scoping the runs, breaking the problem down and validating what actually mattered. The skill that appreciates is thinking like an attacker and knowing your own estate well enough to tell a real threat from a confident-sounding false positive. Tier-1 button-clicking is what the AI is for. The analyst becomes closer to an engineer and an investigator, and the one who decides when the machine's reasoning becomes an action."





CONTINUOUS OPERATIONS, CONTINUOUS RISK

The systems that keep organisations moving are more connected, more regulated, and more exposed than ever.

Cyber Insider tracks the developments behind that shift — from ransomware and critical infrastructure disruption to AI security, cloud exposure, identity risk, regulation, incident response, and supply chain pressure.

Reporting and analysis on the issues shaping cyber risk across UK and European organisations.

cyberinsider.co.uk

CYBER INSIDER

IN CONVERSATION NICK LEEDER, ITI GROUP

New benchmarking data points to a widening productivity and digital capability gap between large and smaller UK manufacturers. We speak with Nick Leeder from ITI Group about why technology alone is not the answer, where SMEs should start, and how a "problems first, platforms second" approach can turn existing assets into measurable operational gains.

Why is the productivity gap between large and smaller UK manufacturers widening?

"The gap is not primarily about technology. It is about management bandwidth, structural disadvantage, and a policy environment built for scale.

"Larger manufacturers have dedicated teams to drive digital projects from pilot to scale and the financial capacity to absorb failure when something does not land. A managing director running a 50-person SME has none of those luxuries. The same person making investment decisions is also dealing with a broken press, a skills shortage and an energy bill that, according to Made in Group's 2026 Industrial Strategy Report, one in four SME manufacturers now describes as survival-threatening.

"The data is stark. Make UK puts UK manufacturing growth in 2026 at -0.5 %. There are roughly 50,000 live vacancies in the sector, costing an estimated £4 billion in lost output. Engineering apprenticeship starts have fallen 40% since the Levy was introduced in 2017, with completion rates as low as 50%. Only 3% of SME manufacturers describe current training programmes as accessible. None of those problems fall more heavily on large manufacturers. All of them compound the disadvantage of smaller ones.

"The SIRI benchmarking programme, drawing on thousands of assessments across more than 60 countries, documents a widening digital divide between manufacturing leaders and the rest. Only 10% of SME manufacturers believe the Industrial Strategy will benefit their business in the next 12 months. Three quarters feel barely or not at all represented in policy. Only 1% find government funding easy to access.

"73% of SME manufacturers are investing or planning to invest in automation and digital within 12 months. The intent is absolutely there. The structural conditions to convert that intent into outcomes, increasingly, are not."

Is the issue really lack of technology, or poor integration of what manufacturers already have?

"The answer to this reflects badly on the technology industry. The challenge is not a shortage of solutions. Manufacturers are not struggling to find vendors. The problem is a shortage of clarity



NICK LEEDER,
STRATEGIC ADVISOR,
ITI GROUP

about problems, and an industry that has spent a decade selling platforms to people who have not yet defined what they are trying to fix.

"The Manufacturing AI Readiness Index 2026 found that cultural resistance ranks at the bottom of barriers to AI adoption, cited by just 3.4% of respondents. The mindset shift has happened. What manufacturers are sceptical about, and rightly so, is return on investment. Lack of a clear ROI was cited by 15.6% as a key barrier. Data quality and availability, the foundational requirement for almost every digital initiative, was flagged by nearly 20% as the most significant obstacle. These are not technology failures. They are preparation failures, and they are a predictable consequence of starting with the platform rather than the problem.

"The WEF Global Lighthouse Network adds weight to this. 86% of business leaders say they are investing in supply chain transformation. Only around a quarter believe their companies have actually completed it. That gap between investment and outcome is enormous, and the availability of technology is not the cause.

"Deloitte found that 92% of manufacturing executives agree smart manufacturing will be the main driver of competitiveness over the next three years. Where it has been implemented well, production output is improving 10 to 20% and employee productivity 7 to 20%. The manufacturers achieving those results are not the ones who bought the most comprehensive platform. They are the ones who defined the problem first. The technology is not the constraint. It rarely has been."



Where should manufacturers start if they want measurable operational gains?

"Start with the data you already have. Most factories are generating more information about their own performance than they are using. It lives in shift logs, maintenance records, quality reports and the knowledge of experienced operators. The question is not whether the data exists. It is whether you have looked at it carefully enough to know which problem most deserves your attention.

"The SIRI benchmarking data identifies the same failure pattern consistently across thousands of assessments in more than 60 countries: a gap between strategic intent and operational execution. Manufacturers set digital ambitions, invest in technology, and find that returns are smaller than expected because the underlying process and organisational conditions were not right. Technology was the third thing that needed to change, not the first.

"The WEF Global Lighthouse Network shows what becomes possible when manufacturers get the sequencing right. Siemens Numerical Control in Nanjing achieved a 50% increase in units per hour and an 83% reduction in delivery lead times through targeted digital twin deployment, grounded in a clearly defined operational problem. Digital twins are regarded as relevant by 86% of manufacturers. Only 44% have implemented them. The distance between believing something is valuable and building the conditions to realise it is where most improvement programmes come unstuck.

"Deloitte's research found that manufacturers implementing smart manufacturing well are reporting output gains of 10 to 20%, employee productivity gains of 7 to 20% and capacity unlocks of 10 to 15%. Not from the most sophisticated technology. From identifying the right problem, establishing a clear baseline, and measuring consistently from day one."

ITI talks about a "problems first, platforms second" approach. What does that look like in practice for a manufacturer with limited budget, legacy equipment, and no large internal digital team?

"It looks like a conversation, not a procurement exercise. It starts with three questions: where are we losing time, where are we losing yield, and where are we consuming resource we should not be? Not in general terms, but with specific numbers attached. If you cannot answer those questions from existing data, that is the first problem to solve, and it is almost always cheaper to address than people assume.

"The Manufacturing AI Readiness Index 2026 found that legacy IT and systems integration is cited as a barrier by 13.6% of manufacturers, and data quality by nearly 20%. Both are genuine constraints, but neither justifies inaction. They are reasons to begin somewhere smaller and more specific than a full platform rollout.

"Legacy equipment is less of an obstacle than it first appears. Condition monitoring sensors do not require replacing anything. They sit alongside existing machines and translate behaviour into useful signals: changes in vibration, temperature or current draw that indicate a component is beginning to fail before it does so. The cost of a sensor is almost always a fraction of the cost of the stoppage it prevents."

How can MES, SCADA, HMI, IoT, and condition monitoring help sweat existing assets?

"Set aside the acronyms for a moment, because they are part of the problem. They make this sound far more expensive and complicated than it is, and they create the impression you need a large, integrated enterprise system before you can get started. You do not.

"What all these technologies share, in practical terms, is a single purpose: they tell you what your equipment is actually doing, and they do so before something goes wrong rather than after. That is the capability that matters.

"Condition monitoring is the most accessible entry point for manufacturers with legacy assets. Nothing gets replaced. A sensor monitoring vibration, temperature or electrical current on a motor, compressor or pump can detect early signs of bearing wear or thermal stress weeks before failure. The cost of that sensor is almost always a fraction of what an unplanned stoppage costs in lost production, emergency maintenance and delivery impact downstream.

"MES and SCADA connect those individual signals into a coherent picture across a production line, revealing where capacity is being lost, why OEE is below target and what the relationship is between process parameters and output quality. HMI puts that information directly in front of the operator who can act on it immediately.

"The WEF Global Lighthouse evidence shows what this delivers at scale. Siemens Numerical Control in Nanjing achieved a 50% increase in units per hour and an 83% reduction in delivery lead times through mature, well-integrated operational technology used with precision. Not the newest system. The right one, connected properly, with the right data reaching the right people."

How should manufacturers measure whether digital projects are actually improving productivity?

"Settle this before the project starts. Not after.

"In practice, that almost never happens. Manufacturers invest, deploy, and then spend months trying to construct a case for the return. The Manufacturing AI Readiness Index 2026 found that nearly 20% manufacturers still report that the value of their digital investment remains unclear within their own organisation. That is not a technology failure. It is a measurement failure, and it begins with

the absence of a baseline.

“Define your baseline and your target metric before any technology is selected. Agree both with the relevant people in the business. If the project aims to reduce unplanned downtime, measure unplanned downtime. If the aim is first-pass defect rate or energy consumption per unit, measure that. One metric, clearly owned, tracked consistently. Not a dashboard of forty indicators that gets opened once and forgotten.

“Deloitte’s 2026 outlook offers a useful benchmark: manufacturers implementing smart manufacturing well are reporting output gains of 10 to 20%, employee productivity gains of 7 to 20% and unlocked capacity of 10 to 15%. Those figures are credible because they were measured against a defined starting point. The discipline of measurement is not administrative overhead. It is what separates an investment that pays back from one that disappears into the business without anyone being able to say what changed.

“Make UK’s growth forecast for UK manufacturing stands at minus 0.5% for 2026. The sector cannot absorb investments that do not demonstrably deliver. If a project has been running for 12 months and you cannot identify a number that has moved in the right direction, one of two things went wrong at the start: the problem was not defined clearly enough, or the implementation was not finished. Both are recoverable. But only if you have been measuring.”



IN CONVERSATION KURT MARKLEY, APRICORN

Apricorn specialises in software-free, hardware-encrypted storage for organisations operating in regulated and security-sensitive environments. Following the company's AS9100 certification, we speak with Kurt Markley, Managing Director, USA, about removable-media risk, the connection between quality and cybersecurity, and the challenge of protecting industrial data across air-gapped systems, remote operations, and complex supply chains.

Apricorn has just announced AS9100 certification. What does that actually mean for customers in aerospace, defence, and other high-assurance sectors?

"On the surface, AS9100 might just seem like another certification, but to those in aerospace and defence it is a significant step. As it's a Quality Management System (QMS) standard, AS9100 serves as a pre-audit for getting devices vetted and procured in these high-assurance sectors. Now that Apricorn is AS9100 certified, the onboarding process in these industries is significantly reduced and it also allows Apricorn to be included in government and defence contracts that demand aerospace-grade quality management systems."

Why should industrial organisations view quality management and cybersecurity as closely linked, rather than as two separate issues?

"Traditionally the two have been seen as separate entities. However, the rapidly evolving cybersecurity landscape is seeing both these disciplines overlap. This is because organisations are realising that IT security can have a huge impact on their quality control systems. If a hacker gains access to their internal quality or reporting systems and makes any alterations, it can have severe implications. For example, if a hacker were to override the cooling protocols at a chemical plant, this could result in a safety incident, so the two are increasingly interlinked."



Removable media can feel like an old problem in a cloud-first world. Why does portable storage still matter so much in today's risk landscape?

"There is no doubt that the world has incorporated the cloud as their go-to for data storage. With that said, the most critical and sensitive systems in the world are often air-gapped. Nuclear power plants, water treatment facilities, and classified defence networks are most often kept from having any physical or wireless connection to the internet, limiting their attack vectors. Those systems still will require updates and the transfer of data, so doing so with removable media is typically the best way to do that. As these systems are very high-level targets, the security posture is enhanced when the removable media is hardware encrypted with some type of anti-virus scan."

Apricorn has focused on software-free, hardware-encrypted devices. What practical advantages does that approach offer in regulated and operationally sensitive environments?

"Hardware encryption certainly has some strong advantages over software encryption. One of the primary differences is that a hardware encrypted drive will typically be OS agnostic, as they do not need to interface with the host for authentication. Software tends to be tied to an OS, be that Windows or Apple, so is then on an attacker's radar. In contrast, a hardware encrypted, software free product, mitigates the potential for malware such as RAM scraping or keyloggers. Also noteworthy is that hardware will typically be faster, as software requires resources from the host to perform the encryption."

From your perspective, what are industrial organisations still getting wrong when it comes to protecting data in transit and at the edge?

"The move to a mostly cloud-centric posture has left many organisations overlooking the edge cases. As mentioned previously, air-gapped systems are still vital to many companies. Many attacks are looking for a trojan horse to those systems, as illustrated by the Stuxnet attacks where a simple, yet compromised, USB flash drive was used on an air-gapped system that led to the destruction of much of Iran's nuclear program. There also a certain amount of overconfidence in air-gapped defence. Just because these systems are not connected to the internet does not make them inherently secure. Many of these are legacy systems that have not been updated, making them easier to compromise if an attacker does gain access.

"Another issue that we see is a heavy reliance on Identity and Access Management (IAM) to keep organisational data safe. If that data is not encrypted, a hacker with stolen credentials can access and potentially manipulate or extract the company's sensitive data. Encrypting that data is one of the best safeguards.

"I would also add that the growing tech stack that organisations are using to safeguard their data can be part of the problem. It can see users become frustrated and resort to work arounds or disable security protocols in order to get their job done and it's something IT Admins seldom understand. So there is a need to consider the impact of implementing "x" technology on work processes and whether it could negatively impact users."



KURT MARKLEY,
MANAGING DIRECTOR, USA,
APRICORN

How are offline workflows, field operations, supplier data exchange, and remote working changing the threat picture for sensitive data?

"I think the pendulum is starting to swing away from the centralisation of all data and workflows. The centralised approach means that a successful attack can potentially provide access to everything. We're seeing more companies move towards decentralising and segregating data.

"It's a trend will bring about a resurgence of 'sneakernet' i.e. the physical transfer of data over storage media rather than via the nework in order to move data around the organisation. This can pose a real risk if those storage devices don't encrypt that data because it could well be intercepted, become lost and/or fall into the wrong hands.

"You mention suppliers and those, especially the smaller sub-contractors, are becoming a prime target for attackers, as they are seen as a weak link.

"With respect to remote work, that's a trend that has really caused many IT managers severe stress. Remote and hybrid workers, even after training, still lean to the path of least resistance. It is much harder to enforce what devices they are using, where they are keeping data or how they are moving it. The company can mitigate that risk by providing clear data storage and backup policies and stipulating which storage devices can be used."

Security teams often struggle to balance protection with usability. What does effective, usable security look like for engineers, contractors, and other non-IT users?

"We hear it often, simplicity is best. When organisations implement security tools that are too complicated or too cumbersome for their users, they inevitably resort to workarounds. The growing tech stack is causing those workarounds to increase. So the organisation needs to do its best to plan around these users or user groups and secure buy-in from them on the solutions being deployed.

"The other option is to get an understanding of what these workflows are, how the security tool is inhibiting the user from their typical workflow, and provide a secure solution for these cases that fits within their abilities. Going forward, the likelihood is that the tech stack will become significantly less complex and move towards more inclusive solutions that target non-IT groups within the organisation to combat this issue."

Shadow IT remains a major concern. What tends to drive it in industrial and regulated environments, and how can organisations reduce that risk without creating friction?

"Remote and hybrid work as well as the increasing tech stack are causing IT managers some real headaches. Most IT admins will admit that there are users utilising their own devices or solutions that have not been vetted by them. And nine times out of ten that's because a user finds the solution that IT has provided too difficult to use, or it slows them down, or gets in the way of their job. It's also a problem that scales so a company with a giant tech stack can, in instances, make it even harder to police the unapproved devices or solutions being used. The average Fortune 500 company's tech stack contains 664+ software applications. You couple managing that with the amount of shadow IT going on, and it's a scenario ripe for exploitation."

How are procurement expectations changing around certifications, compliance, and supplier assurance when organisations buy secure storage products?

"Data security and network security are finally becoming much more ingrained into the minds of IT administrators. Where procurement used to be simply about finding solutions that had "x" certification or validation it's now about digging deeper beyond the check box to ensure that there are processes in place which are being followed. We've seen it ourselves with the more recent supplier/vendor forms. There is much more focus not just on the product that the organisation is purchasing from having "x" credentials – they're increasingly scrutinising the vendor themselves."

Looking ahead, what do you see as the biggest secure storage and data protection challenges facing industrial organisations over the next few years?

"Ransomware and the utilisation of AI will increase the speed and sophistication of attacks and that's already beginning to show. Some of the biggest challenges these organisations will have to navigate include how best to mitigate the employee's role in data security and integrity. This has been the issue for some time and AI will shine a light on that through, for example, phishing campaigns.

"The increasing reliance of organisations on AI could also see them expose a lot of their sensitive data if they are not carefully managing the security around it. Industrial organisations will need to close the gap between their IT groups/directives and their systems and machinery, particularly that managed outside of the IT group's purview. It's a gap that can weaken the security posture of the company at large as the operational group has to be functional for the company to operate and any IT mandates that get in the way of that will likely be avoided."





IN CONVERSATION
PAUL DELLAVILLA, COLD CHAIN TECHNOLOGIES

The pharmaceutical cold chain is no longer just about meeting container compliance standards. Rising shipment risk, tighter regulatory scrutiny, and growing demand for real-time visibility are pushing providers towards predictive analytics, integrated digital platforms, and more sustainable packaging models.

We speak with Paul DellaVilla, Director of Digital Solutions & Services at Cold Chain Technologies, about how data, service-led support, and provider consolidation are reshaping temperature-controlled logistics.

How is the pharmaceutical cold chain market evolving post-pandemic, particularly regarding regulatory scrutiny and shipment risk?

"According to a recent industry survey, 92% of pharma professionals feel that supply chain risk has increased in the past two years.

"This surge in perceived risk stems from a mix of persistent challenges: capacity bottlenecks, regulatory uncertainty and intensifying climate-related disruptions.

"As a result, providers are now expected to collaborate with customers, share insights and co-develop smart solutions to navigate regulatory hurdles, capacity constraints or urgent delivery windows.

"It's also likely that this heightened sense of risk post-pandemic has accelerated the adoption of digital technology. The real-time view and management of shipments as well as predictive analysis provides a sense of security and assurance, even in times of instability."

What role are predictive analytics, IoT asset tracking, and integrated platforms now playing in differentiating providers beyond container compliance?

"The digitisation of cold chain operations is a game changer in terms of compliance, optimisation and real-time visibility. The use of a smart logistics platform offers companies in the cold chain environment the ability to continuously improve, as well as predicting and mitigating potential challenges.

"For that reason, we're seeing data and digital capability become a major decision-making factor for customers. For CCT, centralisation has been a core differentiator. While more and more providers offer some form of digital support, our Smart Solutions platform puts asset tracking such as cellular data loggers (IoT), real time thermal modelling and geofencing technology in one place for complete visibility. Within the same dashboard is predictive modelling and our smart selection engine, along with a whole host of analytics, which means users can see their entire shipping operation in-real time and long term without having to switch between portals.

"We know from customer feedback that this integration and centralisation is a significant contributor to why they choose us as a provider."

How do service-led approaches (like Smart Solutions) improve reliability and risk management compared with traditional compliance-driven models?

"Service-led approaches go beyond traditional compliance by offering the opportunity to assess the likelihood of risk in advance, to plan how to navigate those risks, and to use data modelling to make smarter decisions long term.

"Our Smart Solutions platform allows users to collate data from every shipment, analyse route performance, track regular deviations and monitor thermal behaviour within one dashboard. This offers immediate and long-term risk management benefits. In an immediate sense, the real-time visibility of a shipment means that developing risks can be flagged and resolved before excursions occur. From a longer-term perspective, the centralisation of shipment data allows for the identification of patterns of risk or inefficiencies, allowing for data-driven operational decision making.

"The use of our simulation capability provides another layer of advanced risk management, using real-world data to predict the potential challenges of each route. Plotting a shipment throughout it's journey, including elements like time on tarmac, unplug time and likely ambient temperatures at different stages of transport, means customers can plan for risk and mitigate against it at the very earliest stage.

"With this service-led approach, companies can reduce waste, lower costs, improve reliability and - most importantly - protect product integrity from manufacturer to patient."

To what extent are eco-conscious packaging and resource efficiency becoming a differentiator in temperature-controlled logistics?

"We have certainly seen an increase in customers prioritising sustainability when it comes to temperature-controlled packaging solutions, particularly in the uptake of our multi-use and reusable containers, such as the KTEvolution and EcoFlex.

"Unlike single-use options, multi-use and reusable solutions are designed for durability, with the most robust often lasting over 15 years. At the end of life, many parts of these containers can be reused - and where this isn't possible, there are often measures in place to ensure not a single part of the container ends up in landfill. This longevity and end of life planning significantly reduces packaging waste and lowers the carbon footprint of transportation.

"There are, of course, still applications where multi-use and reusable options are not feasible, but for these, there are now sustainable single use options to mitigate wastage.

"Digital tools such as carbon footprint calculators are able to assess the emissions associated with specific shipments, taking into account variables like container type, PCM temperatures, transportation modes, and payload weights. Life Cycle Assessments (LCAs) can add a further level of detail, providing an overview of the overall environmental impact of the products specified within the supply chain, and therefore informing choices such as which containers are used."

How are pharmaceutical companies assessing providers? Are they prioritising container specs, or broader service and data capabilities?

"There are always a multitude of factors involved in choosing a packaging provider, and it's difficult to choose just one. However, the service offering, both in terms of digital provision and real-world infrastructure is undoubtedly a significant priority for pharmaceutical companies.

"Digital tools and the benefits provided by the real-time monitoring, predictive tools and data modelling offered by integrated platforms are in high demand. Given that the use of these tools can provide financial benefits in the form of product protection and operational efficiencies, as well as enhanced visibility and traceability, it is likely that the emphasis put on digital capability is here to stay.

"However, whilst digital solutions can provide major advantages, there is still considerable emphasis put on human expertise and physical infrastructure.





" Our support structures, for example, help manage challenges such as rerouting critical shipments or troubleshooting temperature excursions, and that sense of partnership can be a major determining factor for customers. Equally, having access to an infrastructure which is able to provide regional support and stock availability globally is important to our customers, as it gives them a sense of security and supports them to meet specific regulatory requirements by region."

Where is cold chain logistics heading in the next five years — greater consolidation among providers, or more specialised service differentiation?

"Consolidation. From a digital point of view, consolidating providers means centralisation of data, which means greater ability to build a full picture of operational efficiency and increased accuracy when it comes to predictive modelling. The use of multiple providers means information is siloed and therefore less useful, reducing the potential benefits of digital all together.

"What's more, the security and trust that comes from a single source relationship is crucial, especially for those shipping high value product. The most advanced cold chain container providers invest in highly specialised technical advisory teams capable of offering neutral, context-driven guidance around packaging selection, risk management, regulatory compliance and thermal strategy – all in the best interests of the customer. Allowing these teams oversight of all shipments offers support to manufacturers throughout the solution lifecycle, from planning and procurement to operations and post-shipment analysis."

PAUL DELLAVILLA,
DIRECTOR OF DIGITAL
SOLUTIONS & SERVICES,
COLD CHAIN TECHNOLOGIES



INDUSTRIAL
NEWS