Issue 3 2025

INDUSTRIAL NEWS

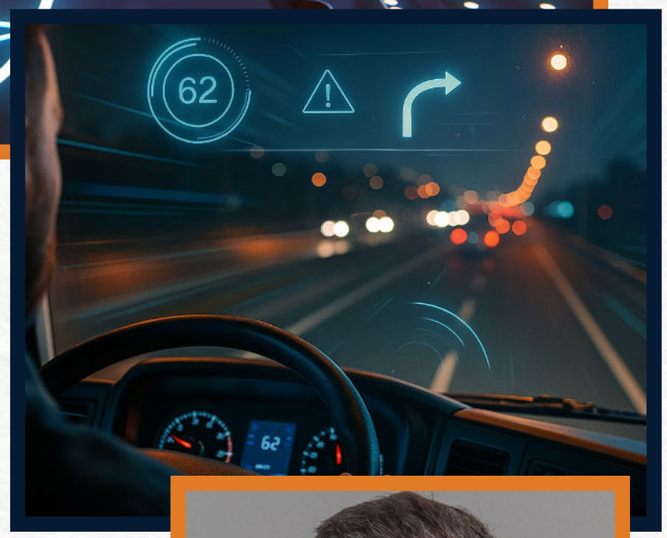
SUPPLY CHAIN RESILIENCE

FROM OPERATIONAL RISK TO BOARD LEVEL PRIORITY

ALSO IN THIS ISSUE

EDGE COMPUTING: WHEN REAL TIME DATA ISN'T FAST ENOUGH

INDUSTRIAL CYBERSECURITY: THE FIRST STEP IS THE RIGHT DRIVE



CONTENTS

INTRODUCTION

Industrial News 4.0 4

IN THE NEWS 6

EDGE COMPUTING

The evolution of industrial automation architectures 12

When real time isn't fast enough 18

Driving supply chain resilience with edge-powered AI 22

IN FOCUS

The supply chain polycrisis 26

CYBERSECURITY

Industrial cybersecurity starts with the right drives 34

Ransomware spikes 49% in first half of 2025 42

COMMENT

***IPP:** IoT–AI combination will be gamechanger* 44

PHARMACEUTICAL

Proactively preparing pharma for the 2030 green supply chain 46

Tightening pharma hygiene to cut contamination risk 50

IN CONVERSATION

*Dael Williamson, **Databricks*** 54

IN BRIEF

You'll notice it straight away — Industrial News looks different. The new logo and refreshed design, are not cosmetic flourishes, but a statement of intent. Industry itself is changing too quickly, too unevenly, and too profoundly for us to stand still.

This rebrand is our response. Industrial News now sits at the centre of a network of specialised titles, each tracking one of the industrial economy's critical pillars.

Welcome to the new Industrial News. Different look. Same purpose.

Jon Hughes, Editor, Industrial News

Editor
Jon Hughes
jon@industrialnews.co.uk

Design
2b Media

Partnerships
Jenn Blakesley
jenn@industrialnews.co.uk

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

Circulation: ~11,200 average
Period: Jan 1st 2024 – Dec 31st 2024

2b Publishing

WELCOME TO INDUSTRIAL NEWS 4.0

Industry today is defined by rapid digitalisation, the acceleration of electrification, and the realities of Industry 4.0 (or 5.0). Manufacturing, energy, supply chains, construction, defence, and food processing are all undergoing transformation, but at very different speeds and in very different ways.

What became increasingly obvious was that a single publication, however comprehensive, could no longer do justice to the sheer scale of progress and the depth of expertise required to cover it. The answer was to expand, and to create specialised titles that could track each sector's upheaval in greater detail — while keeping Industrial News at the centre as the flagship, pan-industrial voice.

As Industrial News steps into its next chapter, the changes are clear on the page. A new logo, a refreshed website, and the launch of a suite of dedicated sub-brand platforms mark a decisive evolution for our publication. These updates are more than cosmetic — they reflect the pace and complexity of change across the industrial world, and our response to it.

Our new sub-brands extend the Industrial News platform into six premium titles, each focused on a critical pillar of the industrial economy.

Alongside these new brands, Industrial News itself will continue to provide the cross-sector view. The industrial economy is no longer a series of silos — technologies, standards, and supply chains converge in ways that no engineer, operator, or policymaker can afford to ignore. Our role remains to chart those connections, to track the industrial themes that cut across borders and sectors, and to deliver IN Depth reports where long-form analysis is needed most.

The changes you see here are part of a broader commitment. Industrial News is expanding not just to keep pace with industry, but to stay ahead of it. We know that our readers operate in a climate where clarity is rare and noise is abundant. Our job is to cut through that noise.

Explore the new sub-brands, subscribe to their updates, and stay with Industrial News for the bigger picture. The landscape is moving quickly. We intend to keep you in front of it.

IN FOOD
PROCESSING & PACKAGING

Covering processing, packaging, automation, and regulation across the food industry, **IN Food** delivers the context needed to navigate one of the fastest-moving manufacturing sectors.

IN SUPPLY
SUPPLY CHAIN & LOGISTICS

Focused on logistics, procurement, and resilience, **IN Supply** examines the technologies, policies, and disruptions shaping how goods move around the globe.

IN SITE
BUILDING & CONSTRUCTION

From advanced materials to digital project delivery, **IN Site** provides construction leaders with the insight to manage and build smarter, faster, and more sustainably.

IN ELECTRONICS & DESIGN

Freshly rebranded from Electronics & Engineering, **IN Electronics & Design** is built for electronics and design engineers and innovators driving the next wave of technology.

IN DEFENCE

Covering aerospace, military systems, procurement, and cyber, **IN Defence** connects professionals with the technologies and programmes shaping modern security.

IN POWER

Exploring electrification, transmission, storage, and grid resilience, **IN Power** addresses the engineering challenges of building reliable and sustainable power systems.

INDUSTRY

ELEMENT MATERIALS TECHNOLOGY UNVEILS MOBILE EMISSIONS MONITORING SOLUTION

Element Materials Technology has invested £500,000 in a mobile emissions monitoring solution, deploying state-of-the-art Selective Ion Flow Tube Mass Spectrometry (SIFT-MS) to provide on-site, real-time data. The unit, the first of its kind targeting process emissions in the UK and Ireland, will enter service in August 2025.

The SIFT-MS van can be dispatched to landfills, wastewater plants, and industrial stacks, enabling rapid detection of hazardous gases such as nitrosamines and PFAS. With emissions rules tightening across Europe, Element's mobile system arrives as the Environment Agency pushes for stricter Emission Limit Values.

Mark Elliot, Technical Manager at Element, said: "Having a mobile emissions monitoring unit that can provide real-time results while still maintaining the laboratory-quality accuracy means businesses can react far quicker if they are falling outside of the limit."

The development marks a significant step in adapting industrial monitoring to stricter environmental regulation.

NOKIA STUDY SHOWS RAPID ROI FROM PRIVATE WIRELESS

Nokia's 2025 Industrial Digitalization Report, produced with GlobalData, finds 87% of enterprises adopting private wireless and on-premise edge saw a return on investment within one year. The study, covering 115 industrial organisations across five countries, also shows reduced setup costs for 81% of adopters and lower ongoing costs for 86%.

The combination of private wireless and edge computing is enabling AI-driven use cases in 70% of deployments, ranging from predictive maintenance to digital twins. BASF's Antwerp site has used Nokia's private 5G to enhance automation, improve safety, and reduce environmental impact across its six-square-kilometre facility.

David de Lancellotti, Vice President of Enterprise Campus Edge Sales at Nokia, said: "GlobalData forecasts the global private wireless network market will nearly double to US$8 billion by 2027. This reflects the growing demand as industries face mounting pressure to modernize in line with global sustainability and efficiency goals."

Beyond environmental impact, 71% of surveyed companies are actively deploying connected worker tools such as automated alarms, AI-assisted monitoring, and geofencing solutions to reduce accidents and strengthen worker safety.

MANUFACTURING SECTOR GROWTH STAGNATES IN Q2 AMID ONGOING UNCERTAINTY

New analysis from **Interact Analysis** shows the global manufacturing sector struggling to gain momentum, with growth stagnating since Q1. Its latest Manufacturing Industry Output Tracker attributes the slowdown to trade policy uncertainty and the ongoing impact of US tariffs. Despite this, global manufacturing output is projected to rise 2% in 2025, driven mainly by China and the United States, while Europe is set for contraction.

In Europe, established industrial economies including Germany, France, the UK, and Italy remain flat, but smaller markets such as Poland, Spain, and the Czech Republic are on track to expand their share into the next decade. Across Asia-Pacific, semiconductor hubs are benefitting from AI-driven investment and supply chain diversification. In the Americas, nearshoring activity presents growth opportunities, but the trajectory remains tightly tied to the US economy.

For the machinery sector, two headwinds are evident. Elevated interest rates have slowed production, creating excess inventories and triggering a destocking cycle. This has coincided with a pause in capital investment as manufacturers await clarity on tariff regimes. While some front-loaded orders were placed ahead of deadlines, Interact Analysis expects new machinery demand to weaken as tariffs bite.

Jack Loughney, Lead Analyst for the MIO Tracker, commented: "The economic uncertainty caused by tariffs has put a dampener on what could've been a good year for the global manufacturing. Despite this, we still expect 2.1% growth in 2025."

Interact Analysis' tracker covers 102 industries across 45 countries, combining 18 years of historical data with five-year forecasts. While near-term output is constrained, the firm points to opportunities in AI-driven investment, regional diversification, and smaller emerging manufacturing economies gaining traction against established industrial centres.

ELECTRONICS

DECA AND SST PARTNER ON NVM CHIPLET SOLUTIONS

Deca Technologies and **Silicon Storage Technology (SST)**, a subsidiary of Microchip Technology, have announced a strategic collaboration to accelerate adoption of non-volatile memory (NVM) chiplets for multi-die architectures.

The partnership integrates Deca's M-Series™ fan-out and Adaptive Patterning® with SST's SuperFlash® embedded flash, delivering a modular, memory-centric package that simplifies chiplet design, verification, and commercialization. The offering includes interface logic, redistribution layer design rules, simulation flows, test strategies, and qualified manufacturing paths.

Robin Davis, VP of Strategic Engagements & Applications at Deca, said: "Our partnership with SST empowers customers to develop a chiplet solution that combines different chips, process nodes, sizes and even die from multiple foundries delivering more efficient and cost-effective products."

Mark Reiten, Vice President of Microchip's licensing unit, added that demand for chiplet-based solutions is rising as companies seek IP reuse, heterogeneous integration, and a practical route beyond Moore's Law.

BITTWARE LAUNCHES EARLY ACCESS FOR 3U VPX CARDS

BittWare, a Molex company, has opened an early access program for its upcoming 3U VPX cards powered by next-generation AMD Ryzen™ Embedded processors, Versal™ RF Series, and Versal Adaptive SoCs. The portfolio, due later this year, targets aerospace and defense applications requiring rugged, compact, high-performance computing for avionics, radar, electronic warfare, and UAVs.

Craig Petrie, Vice President at BittWare, said: "The opportunity to leverage BittWare's proven design expertise along with AMD technology leadership will prove invaluable in giving customers more complete, interoperable solutions to meet ever-increasing demands for compact, rugged designs and highly reliable performance."

AMD's Minal Sawant added that the collaboration will accelerate adoption of adaptive SoCs and embedded x86 CPUs in defense systems. The initiative aligns with SOSA and VITA standards, with complementary 3U VPX power supplies from AirBorn, another Molex company, extending deployment options for mission-critical systems in harsh environments.

CONSTRUCTION

BIOS MATER PROJECT TARGETS LOW-CARBON CONSTRUCTION

A European consortium led by CIRCE has launched **BIOS MATER**, a Horizon Europe initiative co-funded by the EU and the Circular Bio-Based Europe Joint Undertaking (CBE JU). The project aims to replace conventional construction materials with bio-based, circular, and safe alternatives that reduce the sector's carbon footprint.

Bringing together 22 partners from 10 countries, including AIMPLAS, the Plastics Technology Centre, BIOS MATER will develop four new products: bio-based sandwich panels, thermoplastic wall and flooring panels, fibre-reinforced cladding, and biodegradable interior tiles. These will be tested at a dedicated DEMOpark under real-world conditions to prove durability, scalability, and environmental performance.

Carlos Pérez, Project Coordinator at CIRCE, said: "It is truly inspiring to see partners from all over Europe working towards the same goal: to decarbonize the construction sector by applying principles of the bioeconomy and circular economy."

The project directly supports the EU's climate neutrality and Green Deal goals.

COWI TRIALS E-DNA FOR SUSTAINABLE INFRASTRUCTURE

COWI has partnered with the University of Strathclyde to trial environmental DNA (eDNA) as a faster, more accurate method of measuring Biodiversity Net Gain (BNG) for infrastructure projects. The pilot, funded by COWIfonden, is being tested on UK railway sites and could be applied across global transport, energy, and urban developments.

By analysing soil samples for traces of DNA shed by plants, animals, and microbes, the project aims to overcome limitations of traditional ecological surveys, which are often labour-intensive and seasonally constrained. eDNA offers a richer, year-round picture of biodiversity, potentially cutting delays and reducing costs for developers.

Andy Sloan, EVP at COWI UK & International, said: "This partnership with the University of Strathclyde is a practical step in realising our ambition, applying innovative tools like eDNA to improve how we assess and protect nature in infrastructure delivery."

POWER

NEODYNE POWERS UK GRID WITH 50 MW BATTERY PROJECT

NeoDyne, in partnership with **Schneider Electric**, has completed the 50 MW Botley Battery Energy Storage System (BESS) in Hampshire, providing stable renewable electricity to the National Grid and supporting the UK's 2050 net zero target. NeoDyne delivered the electrical design and SCADA monitoring, while Schneider's digital twin and automation solutions enabled real-time visibility and fault diagnostics.

Matt Close, Head of UK Operations at NeoDyne, said: "Delivering the Botley BESS project is a testament to our team's technical strength and commitment to future-proofing industry." The project highlights the partners' growing collaboration in clean energy and automation.

WATTSTOR DEBUTS ATS TO CUT DIESEL RELIANCE

Wattstor has launched Wattstor ATS, an automatic transfer switch that enables commercial and industrial sites to use existing battery storage systems for backup power, reducing reliance on diesel generators. Designed for facilities lacking the budget or space for traditional UPS setups, the system provides a cost-effective resilience solution for mid-sized organisations.

Kevin Ball, Chief Commercial Officer at Wattstor, said: "More and more mid-sized facilities are turning to battery storage to lower energy bills and manage peak loads, and Wattstor ATS allows them to extend that same infrastructure to provide backup power."

Capable of supplying up to 1 MW, the system integrates with Wattstor's Podium EMS, prioritising critical loads and making clean resilience practical for schools, care homes, and light industry.

FUNDAMENTALS LAUNCHES SMART VOLTAGE CONTROL RELAY

Fundamentals has introduced the SuperTAPP SG Essential relay, a new automatic voltage control (AVC) system designed to give industrial and private network operators affordable, scalable voltage management. Built on three decades of SuperTAPP technology, the relay delivers reliable, automated voltage regulation for sites with variable loads and supply conditions, helping reduce risks and maintain performance.

The modular system supports upgrades, flexible deployment options, and applications across manufacturing, renewables, healthcare, transport, and defence.

FOOD PROCESSING

ADVANCED MOISTURE SEPARATORS FOR FOOD PROCESSING

PSB Industries' advanced line of Moisture Separators is engineered to deliver high-efficiency aerosol removal and enhance gas and liquid purity across food processing systems. Designed for adaptability and reliability, the range addresses diverse operational needs while minimising maintenance requirements.

The Centrifugal Separator removes aerosols down to 10 microns, making it particularly suited for high-velocity gas flows in food drying and packaging. Built for durability, it eliminates the need for internal component replacement, reducing downtime and costs.

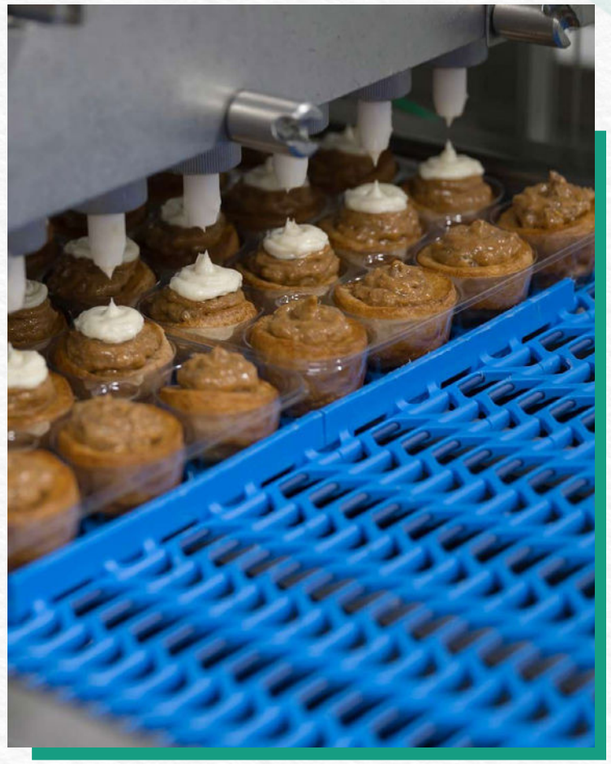
For lower flow rates requiring finer precision, the Demister/Mesh Separator achieves filtration down to 0.3 microns. Its configurable mesh—available as permanent or replaceable—supports excellent turndown capabilities, maintaining efficiency under variable conditions and ensuring consistent performance.

By guaranteeing cleaner air and gas outputs, PSB's separators provide food manufacturers with robust, low-maintenance solutions that enhance process quality, reduce risks, and safeguard the integrity of food production environments.

FINEDALE FOODS SECURES RED TRACTOR ACCREDITATION

Norfolk-based manufacturer **Finedale Foods** has received Red Tractor accreditation, enabling it to source assured meat and meet the scheme's strict processing standards for contract manufacturing clients.

The certification adds to existing BRCGS and RSPO credentials, reinforcing Finedale's focus on responsible sourcing and safe production. The company specialises in chilled and frozen foods, supplying retailers, foodservice distributors, private label brands, and the travel sector.



THE EVOLUTION OF INDUSTRIAL AUTOMATION ARCHITECTURES

*By Dave Sutton, Product Marketing Manager for Industrial Automation, **Schneider Electric***

While every manufacturer is different and leverages digitalisation to achieve individual goals, there are certainly some shared goals applicable to the entire sector. Namely, minimising downtime, improving operational efficiency, reducing waste (in all forms), and contributing to the collective sustainability journey of manufacturing. These goals present challenges that are driving changes in the nature of Industrial Automation control systems towards open architectures at an Operational Technology (OT) level. This evolution can deliver value to businesses and their supply chains.

So, what has been driving the need for open automation? The need to overcome the drawback that although traditional proprietary technologies work well individually, they are locked and closed, with code that is not portable.

It is not feasible for manufacturers to immediately replace critical assets as soon as a more advanced version is available. This leaves legacy hardware in place with bespoke software, communications, and hardware, locking users into one vendor. Typical manufacturers with disparate systems from multiple vendors will see this challenge magnified as they advance in digital transformation. Many end users will require substantial industrial automation (IA) system re-engineering as code written to run on legacy hardware is not portable or compatible with new-generation hardware. This hinders the digital transformation of UK manufacturing, holding back capabilities that will improve efficiency behind large cost and time investments.

The answer is to transition to open automation, as is commonly seen in the IT world. Manufacturers are demanding systems that are software centric and hardware agnostic, so that application code is portable to run on a wide variety of hardware from any vendor. This opens communication across different machines, devices, and sensors, enabling operators to work more efficiently and achieve more with less.

This can be achieved by adopting the IEC 61499 universal automation standard, which is a technology enabler defining how to design distributed applications using ‘plug and produce’ software components independent from the hardware on which they execute. The standard is being led by a community of automation users, technology vendors and academics who want to change the game of automation through the non-profit organisation, Universal Automation.Org.

Plant engineers, systems integrators, OEMs, or anyone involved in the manufacturing supply chain, who design, link and support legacy systems can reduce the massive spend associated with servicing individual assets while setting a pathway for continuous improvement.

For example, in a mature industrial sector such as food and beverage manufacturing, it is common to see a mix of new and legacy assets. A challenge for food processors is that consumers base their purchasing decisions on multiple factors, always looking for the next product or flavour in the fast-moving sector. Manufacturers need to be flexible and scalable to respond to the needs of the market, but this can seem impossible when battling proprietary systems. Open automation enables that level of flexibility with less time spent on non-value-adding tasks and more time innovating.

This example can be applied to manufacturers of any size, producing any product, as shown in our recent research paper entitled ‘A quantitative comparison of digitised industrial automation’. This covers the results of field tests showing that software engineering can be delivered three times faster through open automation for standard production strategies, actively increasing flexibility.

Industrial automation systems currently in operation in UK manufacturing were often put in place decades ago. They’re now holding back manufacturers from realising the full potential of digital transformation and the advances in technologies and computing power. The drive for hardware-agnostic platforms presents an opportunity to use industrialised PCs to run operational application code. This development enables the adoption of soft PLCs or Edge controllers, which

• • •

further fuels the convergence of IT and OT. However, even with manufacturers investing in edge computing technologies to handle the burden of collecting, analysing, and reporting data, the benefits will be limited without an open automation approach that can handle data in a single agnostic platform.

DIGITALISATION

Across industry, we can see wide adoption of IIoT (industrial internet of things) technologies that offer an immediate improvement for manufacturers but ultimately many are held back from realising true potential due to being unable to fully commit to automation.

For example, adding a sensor to a legacy asset for real-time data collection will reduce downtime by supporting proactive maintenance but is limited without interoperability.

Sharing that same sensor data via an open automation platform extends that proactive maintenance capability through access to data from all sources in the facility, new and legacy. The manufacturer can use that single digital thread to make informed business decisions to enhance uptime, maintenance, and energy consumption without the costly investment of new critical assets.

Unlocking the flow of data throughout a manufacturing facility has driven the deployment of more devices at the network edge. This delivers processing power near the assets to create a distributed architecture that offers increased resilience, availability and maintainability. In comparison, traditional large, centralised control

architectures are less able to handle the complexity of modern manufacturing processes, especially as those businesses look to scale and remain flexible.

This has created a growing demand for physical I/O that must be prepared for the data-driven future. A future-ready I/O offering supports universal automation by using open Ethernet protocols to deliver connectivity to a variety of devices and architectures for better performance and availability. Not only will this offer advantages in the short term, it fulfils a promise of universal automation by creating a unified framework for all automation, meaning that architectures created today can evolve with future technologies, once again empowering manufacturers to freely explore any element of digital transformation.

CYBERSECURITY

Any industrial activity that relies on data connectivity will always come with a cybersecurity concern and this isn't reserved only for critical infrastructure. Businesses of all sizes are being increasingly targeted and as manufacturers become part of more complex supply chains the attack surface increases.

Just as universal automation is all encompassing so must be cybersecurity, with a strategy that integrates people, technology, and operations. Just because the flow of data has been opened it doesn't mean there has to be data protection gaps, even with legacy assets that may have exploitable control systems. This has driven the need for solutions that are certified by the IEC62443 cybersecurity

standard to safeguard potential vulnerabilities in industrial systems while providing clear guidance on the responsibilities for every level.

Realising the potential of universal automation and digital transformation, means cybersecurity must be considered beyond processes and procedures to encompass every asset or product that is added to the network.

By decentralising and adopting advanced features, manufacturers will see secure data exchange that reduces risk and improves overall resilience, even as cyber-attacks become more complex. This is essential for manufacturers that want to see the benefits of universal automation with minimised risk, always considering the needs of the future while unlocking immediate benefits.

HIGH AVAILABILITY ARCHITECTURE

Unscheduled downtime represents a massive cost for manufacturers of all sizes. The Performance in Focus 2024 report shows that average hourly cost of downtime stands at £5,471.95 drives the need for predictive maintenance and the open automation that enables it.

To address this challenge, and facilitate high availability architectures where downtime cannot be tolerated, manufacturers can use a mix of technologies such as hot-standby processors, redundant switches, redundant I/O, redundant power supplies, module hot-swapping, Change-Config-On-The-Fly (CCOFT), Fast Device Replacement (FDR) built-in diagnostics, and ring network topology.

Open and universal automation represents the future of industrial architectures, supporting manufacturers as they seek to achieve more with less in 2025. The future-ready approach empowers facilities of all sizes and specialisms to continuously innovate and optimise, looking far beyond single technology deployments and realising the full potential of digital transformation. Universal automation is playing an increasingly important role in UK manufacturing as it continues to digitalise its operations in order to compete on a global scale.

www.se.com

Dave Sutton, Product Marketing Manager - Industrial Automation, **Schneider Electric**

WHEN REAL TIME ISN'T FAST ENOUGH

By Jon Hughes, Editor

Autonomous emergency braking systems have less than 100 milliseconds to detect an imminent crash, process sensor data, and apply the brakes. A late response is not a performance dip — it is a collision. That's the backdrop against which BlackBerry's QNX division has launched its latest operating system, QNX OS for Safety 8.0, a microkernel-based platform built to guarantee that safety-critical functions meet their deadlines without fail.

QNX's move highlights a wider truth across industries now pushing intelligence to the edge. Speed alone is meaningless without guarantees. A system may run blisteringly fast under average conditions, but in safety-critical contexts the only metric that matters is determinism — the certainty that a critical task will always complete on time.

General-purpose operating systems such as Linux, Windows, or Android were never designed with that burden. Their schedulers optimise for throughput and fairness, ensuring multiple workloads share resources efficiently. That philosophy is acceptable in a smartphone or desktop, but catastrophic in a braking controller, a medical infusion pump, or a high-speed production line. A single missed deadline in those contexts constitutes system failure.

DETERMINATION AS THE FOUNDATION

This is where real-time operating systems have carved out their role. Unlike general-purpose platforms, a hard RTOS enforces strict priority scheduling and bounded latency, providing mathematically provable guarantees that critical tasks will execute within their deadlines. The architectural philosophy is different: determinism is the primary design goal, not a by-product.

QNX embodies the microkernel approach. Its architecture strips the kernel back to core scheduling, inter-process communication, and basic memory management, isolating drivers and services in user space. A fault in a network stack or graphics module cannot cascade into brake control or a medical monitoring loop. That isolation, along with a smaller trusted code base, makes formal verification and safety certification more achievable. It is why QNX has become the market incumbent in automotive, embedded in more than 255 million vehicles worldwide and serving as the foundation for 24 of the top 25 electric vehicle manufacturers.

By contrast, monolithic kernels such as Wind River's VxWorks integrate all services in a single address space. The upside is performance — direct calls between components avoid the overhead of context switching — but the trade-off is fragility. A fault in one driver can corrupt the entire system. That model still dominates parts of aerospace and defence, where performance has historically outweighed verification concerns, but microkernels have gained ground as certification demands have tightened. Green Hills Integrity has pursued a separation kernel strategy for similar reasons, positioning itself in aerospace and defence projects where partitioning is mandatory under standards such as DO-178C.

MILLISECONDS MATTER

The certification landscape has become the critical driver. ISO 26262 in automotive, IEC 61508 in industrial automation, IEC 62304 in medical devices, and DO-178C in aerospace all demand not only deterministic performance but demonstrable isolation and fault containment. Here, QNX and its peers package their operating systems as "pre-certified" foundations, supplying the artefacts and safety cases needed to accelerate regulatory approval. Attempting to certify a sprawling Linux distribution for an ASIL-D or DAL-A function is financially prohibitive; relying on a safety-certified RTOS is the only viable route to market.

The use cases speak for themselves. In advanced driver assistance systems, dozens of concurrent tasks — from ingesting radar and camera feeds, to fusing them into a coherent world model, to calculating time-to-collision, to actuating the brakes — must all execute within a strict budget. A deterministic scheduler is the only way to guarantee this deadline is consistently met, which is why QNX has made this sector its home ground.

INDUSTRIAL NEWS

In medical technology, the problem is different but equally unforgiving. A smart infusion pump must drive a motor at precisely timed intervals while simultaneously monitoring sensors for blockages or stalls. Jitter in this loop can result in under-dosing or overdosing a patient, and any delay in raising an alarm can be fatal. Using a general-purpose OS here would categorise the entire platform as “software of unknown provenance,” forcing the manufacturer to assume an impossible validation burden. Deploying a certified RTOS such as QNX or SafeRTOS provides a clear path through IEC 62304 Class C compliance.

Industrial automation presents another case. Programmable logic controllers on packaging lines must execute control cycles within millisecond ranges. A delayed signal can damage machinery or injure operators. Once again, determinism is the difference between a clean stop and an incident report.

A hybrid future

The global RTOS market was worth around USD 7 billion in 2023 and is projected to grow at nearly 8% annually, with automotive autonomy as the prime engine. Consumer IoT still accounts for most unit volumes, but the value is in certified hard RTOS deployments — the ones that underpin cars, aircraft, medical devices, and factories.

The future is likely to be hybrid. Modern systems-on-chip now consolidate dozens of functions of varying criticality, and the only way to manage them is to split responsibilities. A safety-certified RTOS runs in one partition, handling deterministic control loops, while a general-purpose OS such as Linux or Android runs in another, managing user interfaces, AI, and connectivity. QNX has explicitly engineered its 8.0 release for this model, optimised to coexist alongside feature-rich operating systems while maintaining its safety certification boundary.

When it comes to safety, speed without guarantees is meaningless. Determinism, certification, and isolation define whether an embedded system is trustworthy. QNX’s latest release is only the most recent example, but it illustrates the broader reality: as industries converge on ever more software-defined architectures, the operating systems at their core are no longer an afterthought. They are the foundations upon which safety — and regulatory approval — rests.

www.blackberry.qnx.com/en

DRIVING SUPPLY CHAIN RESILIENCE WITH EDGE-POWERED AI

By Jeremy Coleman, Associate Director, ***Netradyne***

A supply chain is only as strong as its weakest link, and for many organisations, that link is the road. Warehouses, port strategies and inventory planning get attention, but fleet-level resilience is often overlooked. The most immediate and unpredictable disruptions, from sudden accidents to extreme weather, happen on the road.

In modern fleet operations, analytics play a central role in monitoring everything from vehicle performance to driver behaviour. These insights help fleet managers make data-driven operational optimisation, and improve safety protocols. But when every second counts, traditional cloud-only analytics can fall short.

Operators need a faster and more autonomous form of intelligence, one that can act in the moment without depending entirely on remote servers. This is where edge-powered AI is making its mark on fleets, enabling drivers to detect and respond to risks instantly before they cause issues that can impact the entire supply chain.

THE CLOUD'S LATENCY PROBLEM

Cloud-based fleet systems shine in large-scale optimisation, but in split-second road scenarios, latency can be costly. When network connectivity falters or bandwidth lags, analytics delays jeopardise safety. Waiting for cloud insights is simply too slow to prevent critical incidents in real-time.

Cloud-only systems depend on continuous connectivity, and if a vehicle enters an area with poor coverage or network congestion, the delay between capturing data and receiving a response can compromise safety. Even with a strong signal, the round-trip to the cloud takes time, and in high-stakes situations, seconds matter.

WHAT EDGE COMPUTING BRINGS TO FLEET SAFETY

Edge computing vision systems powered by artificial intelligence, on the other hand, bring an additional dimension to fleet resilience. By processing road-level data at the point of capture, they deliver immediate awareness of traffic patterns, driver behaviour and environmental risks. This transforms the road from a potential point of disruption into a continuous source of operational intelligence.

For fleets managing large numbers of vehicles, often completing multiple deliveries a day, this insight also supports cost control. Transport operations represent a significant share of logistics spend, and small improvements in routing, driving style and incident prevention can translate into considerable savings across a network.

Indeed, edge AI's value extends far beyond safety. By analysing driving patterns such as braking, acceleration, and route choices, it can help fleets uncover operational inefficiencies that, once addressed, can reduce costs and boost vehicle uptime.

The measurable impact can be substantial. For example, logistics provider Load One Transportation reported a 59% reduction in insurance claims within a year of introducing an edge-powered, AI-driven fleet safety system.

The ability to analyse 100% of drive time, rather than isolated events, further enhances decision-making. With a complete view of drive time, fleet

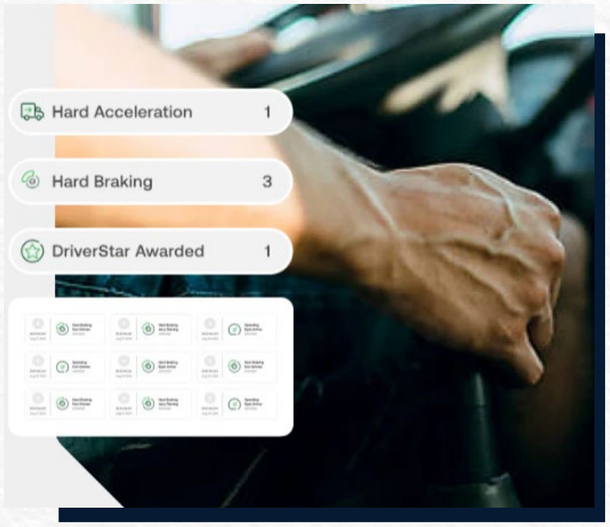
managers can identify patterns, address recurring risks and provide targeted coaching that supports long-term performance improvement. For supply chain leaders, adopting real-time road intelligence through AI-powered edge vision systems is not just a safety measure but a strategic advantage for visibility, adaptability and risk management.

RESILIENCE WITHOUT RELIANCE

Operational continuity is an area where edge-powered AI proves invaluable. In transport and logistics, losing connectivity can be a regular occurrence, particularly during long-haul, rural or cross-border journeys. When decision-making happens in the cloud, these interruptions can leave vehicles without critical safety functionality.

By processing data locally, fleets can maintain hazard detection, driver coaching and decision-making without interruption, even when the network drops. Once connectivity is restored, the data synchronises with central systems to keep records complete and consistent.

This localised approach supports stronger data privacy and compliance. With regulations tightening around how personal and operational data is collected, stored and transmitted, keeping sensitive data on the device reduces exposure and supports regulatory compliance. Only the insights needed for centralised management are transmitted, limiting the risk of breaches and ensuring that safety improvements do not come at the expense of responsible data practices.



PREDICTIVE RISK DETECTION AND REAL-TIME COACHING

One of the most significant applications of edge-powered AI in logistics is predictive risk detection. AI models, trained on millions of driving scenarios, can constantly monitor the driving environment, assessing traffic flow, vehicle dynamics and road conditions to identify potential risks before they escalate. If a hazard is detected, the system can deliver an immediate alert to the driver, enabling swift corrective action. This transforms safety from a reactive process into a genuinely proactive one, preventing incidents rather than simply responding to them.

A further critical benefit is the ability to provide real-time driver coaching. Traditionally, feedback on driver behaviour has been delivered retrospectively, often hours or days after a journey. While useful, it does little to prevent incidents in the moment. With edge processing, feedback can be provided instantly. If risky behaviours such as speeding, tailgating, jumping traffic lights, drowsiness or distracted driving are detected, the system can issue prompts to the driver to correct them immediately. Over time, this creates a continuous feedback loop that encourages safer driving habits and strengthens a safety-first culture across the fleet.

For example, Kutzler Express, a US-based YMX Logistics company, has implemented Netradyne's video-based fleet safety solution in its vehicles. In just one year, they have seen significant results in every area of the business, from improved driving performance to faster exoneration in not-at-fault incidents.

Of all the variables that can derail fleet operations, safety remains the most unpredictable and consequential. Research demonstrates that human error accounts for over 70% of road accidents, with these incidents costing employers nearly $60 billion annually. Safety represents the ultimate operational wild card - one that traditional reactive approaches simply cannot adequately address.

Edge-native AI solutions process safety-critical data instantaneously at the vehicle level. Industry adoption patterns suggest this technological convergence is rapidly becoming essential rather than optional. Currently, 32% of fleet managers recognise AI as the most significant operational game-changer, with 35% planning implementation within the next five years.

This acceleration is being driven not just by competitive advantage, but by evolving regulatory expectations that increasingly demand proactive safety management.

By 2028, as global fleet management markets reach $75.5 billion, the competitive differentiator will not be whether organisations have adopted these safety intelligence technologies, but how effectively they've integrated them into proactive operational frameworks. The future belongs to fleet managers who can predict the unpredictable.

www.netradyne.com/uk

Jeremy Coleman,
Associate Director,
Netradyne

THE SUPPLY CHAIN POLYCRISIS

Why supply chain resilience is rapidly becoming a board-level issue

By Jon Hughes, Editor

In September 2025, a ransomware attack forced Jaguar Land Rover to halt production at several UK plants, with disruption spreading to suppliers and schedules. For industrial operators, the lesson was blunt: a single cyber event can shut lines, snarl logistics, and cascade across an ecosystem. Analysts estimate automotive line downtime at ~$22,000 per minute; Dragos logged more than a thousand industrial ransomware incidents in the first half of 2025, with manufacturing the prime target — cyber now sits alongside physical chokepoints as a top-tier operational risk.

That convergence defines 2025's operating reality. Detours and congestion tightened freight conditions as carriers rerouted around conflict, while the Panama Canal's early-year rebound was tempered by longer-term water stress. Seasonal openings along the Central Arctic route added a further variable rather than relief. It is a system where shocks overlap, and one disruption can disguise the impact of another.

"Supply chains continue to operate in a landscape defined by disruption and strategic complexity, with pressures mounting in several critical areas: geopolitical volatility, regulatory shifts, climate risk and cyber threats," says Rasheed Mohamad, Global Revenue and Operations Officer at **Alcatel-Lucent Enterprise**. "What sets today's landscape apart is the convergence of these pressures. They're no longer isolated events, but interlinked stressors that amplify each other."

That poly-crisis is temporal as well as thematic. "While the nature of vulnerabilities differs from sector-to-sector, what's universal is that threats are increasing from all directions for many organisations," says Dr Chris Smith, Senior Lecturer (Associate Professor) in Operations and Critical Systems at **Alliance Manchester Business School**. "In the short term, cyberattacks continue to cause sudden and significant disruption… Medium-term risks could be geopolitical… Longer term, climate change presents a systemic challenge."

The C-suite isn't short of signals. Gartner puts fewer than 29% of supply chains in the "future-ready" bracket; BSI's 2025 MESH report records resilience as a board priority in most companies, yet only 6% achieve a "leading" maturity across mapping, continuity, supplier assurance, and digital integration. Many experienced significant disruption over the past year while continuity plans went untested. The gap between awareness and operational reality remains wide.

THE REGULATORY MATTER

Regulation is turning that gap into immediate commercial risk. Europe's NIS2 extended cybersecurity obligations from October 2024 and attaches significant penalties; CBAM shifts from transitional reporting to financial consequences in 2026; CS3D entered into force in 2024 with national transposition and phased compliance to follow. In the US, UFLPA enforcement has held and seized thousands of shipments across electronics, apparel, and pharma — a direct line from due-diligence failures to revenue loss and reputational exposure.

"There's a notable shift from facilitation to enforcement, influencing how companies manage compliance, customs documentation, and internal audits," says Nick Baker, Managing Director in the Transfer Pricing practice and co-lead of the Trade and Customs practice at **Kroll**. "New tariff regimes and increased audit risks are prompting many firms to rethink sourcing and pricing strategies… Together, these trends are reshaping how firms plan for resilience."

The mechanics bite at the border and in the boardroom. Under NIS2, failures can carry management liability as well as fines; under CBAM, embedded-carbon accounting becomes a cost item; under UFLPA, shipments are stopped unless companies prove provenance. With reporting calendars stacking through 2025–26 and guidance hardening into enforcement, resilience has moved from "ops issue" to fiduciary duty.

The chokepoint picture compounds the pressure. Red Sea rerouting extended transit times and reset rate dynamics; the Panama Canal posted record container transits early in 2025, but the rebound sits on fragile hydrology; Arctic passages are niche, seasonal, and infrastructure-light. Boards are left managing volatility rather than clear substitutes.

"Supply chains that span multiple global hubs – particularly connecting Asia, Europe, and North America – are under the greatest pressure right now," says Amanda Khalaf, UK Partner and Head of Supply Chain Planning at global operations strategy and transformation consultancy, **Argon & Co**. "These networks are being strained by a volatile policy environment… Layered onto this are ongoing conflicts affecting critical trade routes… The situation is especially difficult for businesses without in-house customs or trade expertise… In short, global supply chains are feeling the most pressure as geopolitical uncertainty intersects with deep operational complexity."

That visibility problem is deeper than many leaders admit. "One of the most overlooked lessons from the past year is just how limited procurement visibility still is – especially when it comes to geography," Khalaf adds. "Many companies discovered, often too late, that they lacked accurate data on where their goods are actually manufactured… The companies responding most effectively… are prioritising better data: running targeted impact analyses, launching supplier surveys, and mining existing information to map geographic dependencies more clearly."

FROM CONTROL TOWERS TO COLD CHAINS

The practical playbook is data-first. Digital twins are credited with improving forecast accuracy and cutting delays; AI control towers shrink problem-identification windows from weeks to minutes; additive manufacturing localises risk by putting spares production close to need and stripping inventory bloat from legacy parts. DHL reports twin-driven gains in warehouse efficiency and energy use; Siemens Energy prints on-demand parts for critical equipment; GE Aviation's consolidated fuel nozzle cut weight and cost while simplifying its bill of materials. None of these moves eliminate volatility, but they reduce the blast radius when it hits.

The cyber overlay is unavoidable. Dragos registers industrial ransomware activity concentrated in manufacturing because downtime pays; the Jaguar Land Rover outage shows how OT disruptions propagate up and down tiers. "While global supply chains face pressure from geopolitical tensions and inflation, cybersecurity remains an acute and unpredictable threat," says Marc Wren, OT Cyber Security Manager at MSP **Axians UK**. "The recent cyberattacks on Adidas… and Marks & Spencer… underline the fragility of interconnected supply networks. The issue lies in the interdependence of these ecosystems… A breach at any point… can trigger cascading failures."

Technology helps — but only if it is aligned to business risk. "The continued convergence of Information Technology (IT) and Operational Technology (OT) is transforming how supply chains operate," Wren notes. "Technologies like IoT sensors, AI-driven threat detection and predictive maintenance systems are improving visibility, reducing downtime and enabling proactive decision-making… Unified security teams can now isolate and protect critical systems before ransomware or other threats spread through the network."

The sector view shows why one-size solutions fail. In pharma, flooding at a North Carolina site triggered nationwide IV-fluid shortages in late 2024, exposing thin redundancy in critical medical supply; resilience moves include regional manufacturing options, predictive logistics, and cold-chain telemetry. In manufacturing and engineering, additive production and nearshoring shorten lead times and reduce customs exposure; Siemens Energy's spares-on-demand model and GE's nozzle consolidation are the canonical examples. In med-tech, Dr Amit Gupta's digital-twin experiment across a 21-hospital system demonstrated how to stress-test flows without jeopardising live care.

Strategy matters as much as tooling. "Looking ahead to 2026, the single most impactful shift for supply chain resilience will be adopting a mindset of adaptability over optimisation," Khalaf says. "In a world where disruption is the norm… companies can no longer afford to optimise solely for cost-efficiency… The future belongs to those that embrace scenario thinking – proactively sensing, simulating and adapting to changes… It's not just about internal operations anymore – we need to think in terms of ecosystem orchestration."

The human and governance layers are easy to neglect — and costly to ignore. "Supply chains are only as strong as their weakest (digital) link," Wren warns. "Even companies with robust internal cybersecurity… can fall victim when smaller, third-party vendors lack adequate protections… This calls for a shift in mindset toward shared responsibility… Cybersecurity due diligence, vendor risk assessments and supply chain-wide threat monitoring must become standard practice, not afterthoughts."

For multi-national manufacturers, trade policy volatility remains a force multiplier. "The most intense pressure today lies at the intersection of trade policy, regulation, and logistics," says Nick Baker. "There's a notable shift from facilitation to enforcement… On the technology side, digital tools for supply chain visibility and scenario planning have become essential… A shift from short-term firefighting to long-term scenario planning is essential."

And the board-level mandate is broader than "buy tools." As Alcatel-Lucent Enterprise's Mohamad puts it: "The message is clear: in the next era of global commerce, resilience is not a response – it's a capability. One that must be built intentionally, collaboratively, and continuously."

For managers, the challenge is not only building resilience but also demonstrating its business value in terms that resonate at the top table. That means linking operational changes to measurable impacts: shipment holds avoided, downtime reduced, or regulatory penalties prevented. Scenario drills, supplier mapping, and compliance readiness may be day-to-day exercises, but they translate into board concerns when expressed as cost, liability, or reputation exposure.

Technologies provide another line of argument. Digital twins, AI control towers, and additive manufacturing already deliver reductions in lead times, downtime, and operating cost. Framed in ROI rather than technical novelty, these examples strengthen the case for investment.

Climate forecasting and OT cyber hygiene, meanwhile, are no longer optional "resilience extras." They are the baseline protections managers can present as risk offsets — particularly when benchmarked against sector peers.

The winners over the next 12–18 months will be the managers who can demonstrate resilience not as contingency planning but as a value-creating operating model. Boards may sign the cheques, but it is those in procurement, operations, and logistics who will shape the arguments that get them written.

DIVE DEEPER INTO SUPPLY CHAIN RESILIENCE

Our upcoming IN Supply special report brings together the uncut expert insights, sector case studies, and board-level strategies that didn't fit into this issue's feature.

Sign up now to access the full report when it launches.

INDUSTRIAL CYBERSECURITY BEGINS WITH THE RIGHT DRIVES

By Prabhu Nagavi, Global Product Manager for Machinery Drives, ABB

In the first quarter of 2025, ransomware attacks targeting manufacturers rose by 46%. For many in the industrial sector, this statistic may be alarming, but not surprising. As factories adopt highly connected, intelligent production systems, the same connectivity that powers efficiency and innovation also creates entry points for cybercriminals. The operational technology (OT) layer, which sits at the heart of industrial machinery and processes, is now a critical front line in the fight against cyber threats.

But in too many cases, one essential OT component — the industrial drive — is pushed to the sidelines during cybersecurity conversations. By regulating motor speed and torque to match demand, drives optimise motor performance and act as intelligent links within wider automation networks. If compromised, unplanned downtime, safety risks, product quality issues, and costly production losses are all on the cards. Even more pressing is the fact that a successful attack could breach a plant's entire network through unsecured points in the drive layer. And for small and mid-sized OEMs, the move toward secure-by-design machinery is especially tough, with tight budgets and limited in-house expertise often making it hard to embed security from the very start.

It is no longer enough for manufacturers to address cybersecurity only at the IT network level. To achieve true resilience, protection must be baked directly into the OT assets themselves, starting with drives.

CYBER RISK IN EVERY CONNECTION

In the last decade, industrial automation has shifted from isolated control systems to a fully networked, data-rich ecosystem. Ethernet connectivity is increasingly standard on drives, PLCs, and sensors. Machine builders and plant managers now expect to have real-time visibility and analytics at their fingertips to keep operations running at full tilt.

But this connectivity also opens the door to vulnerabilities, from asset configurations falling into the wrong hands, to outdated firmware or weak authentication protocols offering easy targets for exploitation. Even something as seemingly harmless as a default-open communication port can provide exactly the kind of foothold a cybercriminal needs.

Too often, performance and integration speed take centre stage, and understandably so; but cybersecurity gets left to be handled later. This "bolt-on" approach to cybersecurity is risky. Regulatory bodies, particularly in Europe, are moving to tighten compliance requirements for OEMs, and those that fail to build in cyber protection from the start will leave machines non-compliant and vulnerable.

Recent innovations in drive design point to how the industry is starting to tackle these risks head-on. Take ABB's ACS380-E machinery drive: it's been built with cybersecurity woven into its fabric, rather than stitched on as an afterthought. For small and mid-sized OEMs, this marks a valuable chance to strengthen their designs. By integrating security directly at the drive layer, the foundation of the automation stack, machines can be cyber-secure from

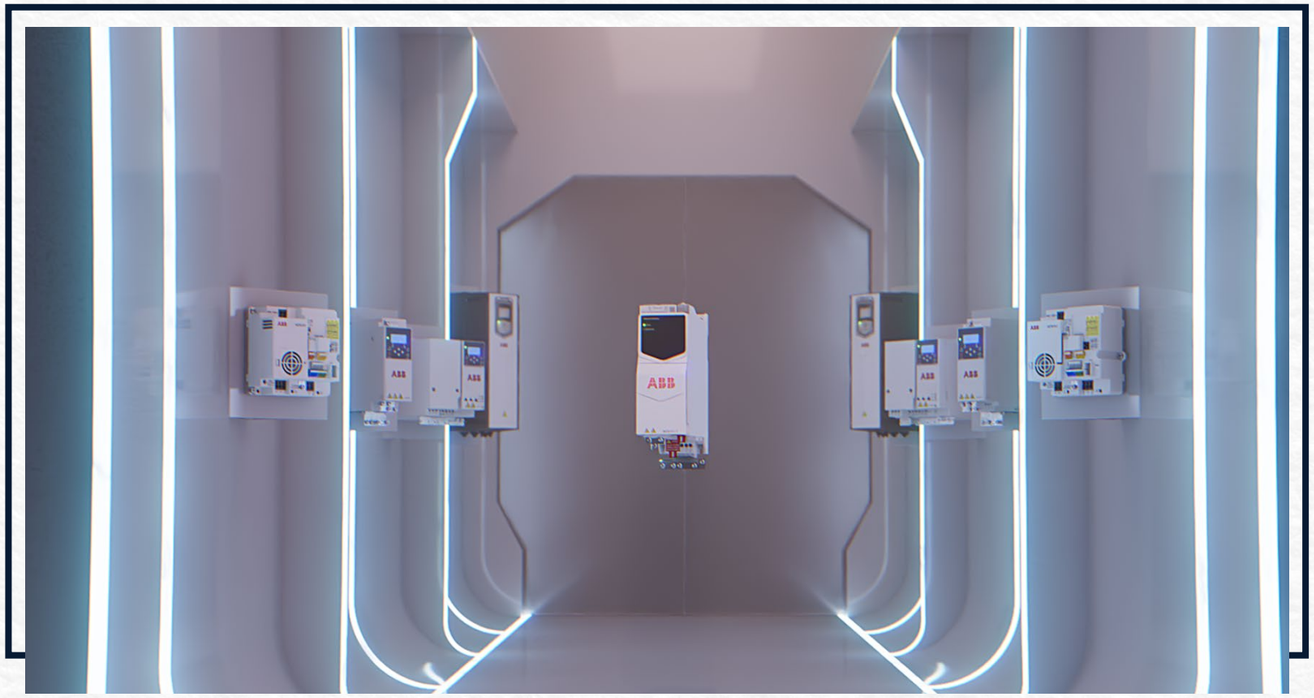
day one without relying on expensive or complex extras. Plus, this kind of foresight can make the difference between meeting the EU's upcoming Machinery Regulation updates in 2027 and rushing to implement last-minute fixes.

Rather than relying on a padlock at the network perimeter, this new breed of drive focuses on safeguarding each connection point and control function from the inside out. Even the supply chain is treated as part of the security perimeter, with hardware-level safeguards to make sure no one can slip in altered components along the way. In today's connected manufacturing world, every device on the network is a potential Trojan horse. The shift toward secure-by-design drives signals a broader industry realisation: if you don't lock down the smallest components, the resilience of the whole system is at risk.

CONTROLLING ACCESS AND CONTAINING RISK

The ACS380-E supports both local and centralised account management, with role-based access that even the manufacturer can't override. It boots only from software it can trust, refusing to run anything that hasn't been signed off, and if tampering is detected, it quietly rolls back to its last clean version without missing a beat.

Those same principles extend to how the drive communicates. By locking connections to trusted devices, unused access points are taken off the table entirely and every attempt to interfere is recorded in a security log. In today's industrial environments, knowing exactly when and how someone has tried to gain access to the network is just as important for compliance and long-term resilience.



THE QUESTIONS TO ASK

Historically, buying a drive often has come down to performance characteristics: speed control, torque accuracy, energy efficiency. While these remain critical, the procurement process must now also account for cybersecurity readiness.

The first question industrial buyers should ask themselves when evaluating a new drive is whether it complies with the relevant standards and regulations for their market. While it's worthwhile to ensure compliance today, it's just as critical to choose solutions built to adapt as new regulations take shape.

Secondly, it's important to check if secure boot processes and signed firmware are standard features, ensuring the drive will only run trusted code. Watertight user authentication is another key consideration, along with the ability to integrate access control into existing security systems.

Built-in monitoring and event logging are equally essential, both for detecting incidents in real time and for providing a record to support investigation and assure auditors. Finally, buyers should establish whether unused access points can be disabled. Closing them before the drive even goes into service cuts down the number of ways an attacker could get in. Drives that do not offer these capabilities will not only be more vulnerable, but it could leave an entire facility falling short of future compliance rules.

In industrial automation, cybersecurity and performance are not separate priorities. Without security, performance gains are fragile and at constant risk, and secure systems enable the reliable operation needed for productivity.

ABB's ACS380-E shows that it is possible to combine advanced motor control and broad connectivity with built-in, standards-compliant cybersecurity. For OEMs and end users, this approach reduces integration effort and boosts confidence that their systems will meet both today's and tomorrow's demands.

The constant flow of news stories around ransomware attacks should be a wake-up call for the entire industrial sector. And since drives sit at the convergence point of operations, machinery, and networks, securing them is no longer optional.

www.abb.com/global/en/areas/motion/drives

Prabhu Nagavi, Global Product Manager for Machinery Drives, **ABB**

5 INDUSTRIAL CYBER CASES TO LEARN FROM

Industrial cyber attacks have become impossible for industry to ignore. Over the past decade, a handful of incidents have gone far beyond IT disruption, halting physical systems, crippling supply chains, and reshaping how governments and businesses think about operational resilience. These five stand as the most consequential... so far.

1 The $10bn wiper (NotPetya, 2017)

What began as a disguised ransomware campaign in Ukraine spiralled into the costliest cyber attack on record. Spread through a compromised update of the M.E.Doc tax software, NotPetya weaponised the leaked NSA exploit “EternalBlue” to propagate uncontrollably. Its true function was not extortion but destruction: encrypting master boot records and rendering systems unrecoverable.

The collateral damage was immense. Maersk’s global shipping operations were paralysed for two weeks, costing up to $300 million. FedEx subsidiary TNT lost $300 million, Mondelez lost $150 million, and pharmaceutical giant Merck reported nearly $900 million in disruption. Total global losses are estimated at over $10 billion.

NotPetya made clear that industrial supply chains are a single, connected system. A compromise at one Ukrainian vendor metastasised into a worldwide industrial catastrophe — proof that resilience cannot stop at organisational boundaries.

2 The first cyberweapon (Stuxnet, 2010)

Discovered in 2010, Stuxnet remains the archetype of the industrial cyber attack. Engineered to cross air gaps via infected USB sticks, it targeted Siemens Step7 software controlling uranium enrichment centrifuges at Iran’s Natanz facility. By subtly manipulating rotor speeds while feeding operators false data, the worm destroyed around 1,000 centrifuges.

Stuxnet was the first malware designed for physical sabotage. Its complexity — four zero-day exploits, advanced stealth, and deep process knowledge — indicated nation-state authorship, later widely attributed to US and Israeli intelligence.

The attack’s significance lies less in Iran’s lost centrifuges than in what it proved: industrial control systems were no longer theoretical targets. The assumption that proprietary protocols and isolated networks offered protection was permanently dismantled.

3 IT disruption, OT shutdown (Colonial Pipeline, 2021)

In May 2021, a criminal ransomware group, DarkSide, gained access to Colonial Pipeline’s corporate network via a compromised VPN password lacking multi-factor authentication. Although the pipeline’s operational systems were untouched, the company shut down 5,500 miles of pipeline as a precaution — halting 45% of the East Coast’s fuel supply.

The operational impact was immediate. Panic buying led to shortages across multiple states, with petrol prices hitting a six-year high.

Colonial paid a $4.4 million ransom, some of which was later recovered by the FBI.

Colonial Pipeline showed that disruption of IT systems alone can have national-scale industrial consequences. The supposed barrier between corporate networks and OT environments proved more porous than protective — and criminals, not just state actors, were now capable of sparking systemic disruption.

4 The SCADA cyber blackout (Ukraine power grid, 2015)

On 23 December 2015, attackers from Russia's Sandworm group manually opened circuit breakers in western Ukraine, plunging more than 225,000 customers into darkness for up to six hours. Access was gained through spear-phishing emails carrying BlackEnergy malware, with operators using stolen credentials to seize control of SCADA systems.

The attack was multi-pronged. KillDisk malware wiped servers and workstations, while a denial-of-service attack crippled call centres, preventing customers from reporting outages. The blackout struck in midwinter, underscoring its potential as a weapon of hybrid warfare.

Ukraine's grid attack proved a long-feared point: critical utilities could be taken offline not only by bombs, but by keystrokes. It remains a touchstone for discussions about energy resilience under geopolitical pressure.

5 Attacking safety systems (Triton/Trisis, 2017)

Discovered at a petrochemical facility in Saudi Arabia in 2017, Triton (or Trisis) targeted Schneider Electric Triconex safety instrumented systems — the last line of defence against hazardous failures. The malware was built to reprogram these controllers, potentially allowing physical processes to run unchecked while giving operators false assurance.

The attack was uncovered only because a handling error triggered a safe shutdown before the payload could be deployed. That failure may have prevented mass-casualty consequences. What makes Triton significant is intent: it was the first known cyber operation designed to disable safety systems directly, opening the door to cyber attacks intended not just to disrupt but to endanger lives.

Taken together, these five incidents mark a progression. Stuxnet introduced sabotage as a viable tactic. Ukraine's blackout confirmed utilities could be switched off at will. NotPetya exposed the global fragility of interconnected supply chains. Colonial Pipeline showed criminals could trigger national disruption. Triton crossed into the realm of safety system compromise.

The lesson is neither subtle nor comforting: modern industry cannot rely on obscurity, isolation, or luck. For industrial operators, resilience means assuming compromise and planning recovery — because the next defining attack is less a question of if than when.

RANSOMWARE SPIKES 49% IN FIRST HALF OF 2025

The number of ransomware attacks in 2025 has almost doubled compared to last year, with US organisations and SMBs as the primary targets.

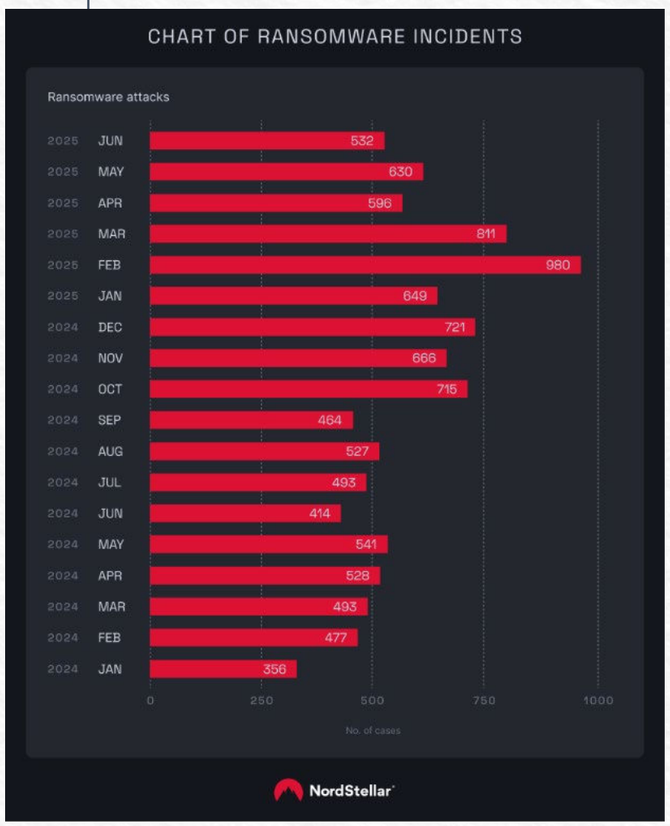
The latest data compiled by NordStellar, a threat exposure management platform, reveals that the number of ransomware incidents has almost doubled compared to last year. In January-June of 2025, 4,198 ransomware cases were exposed on the dark web, highlighting an alarming 49% increase from the 2,809 cases recorded in 2024.

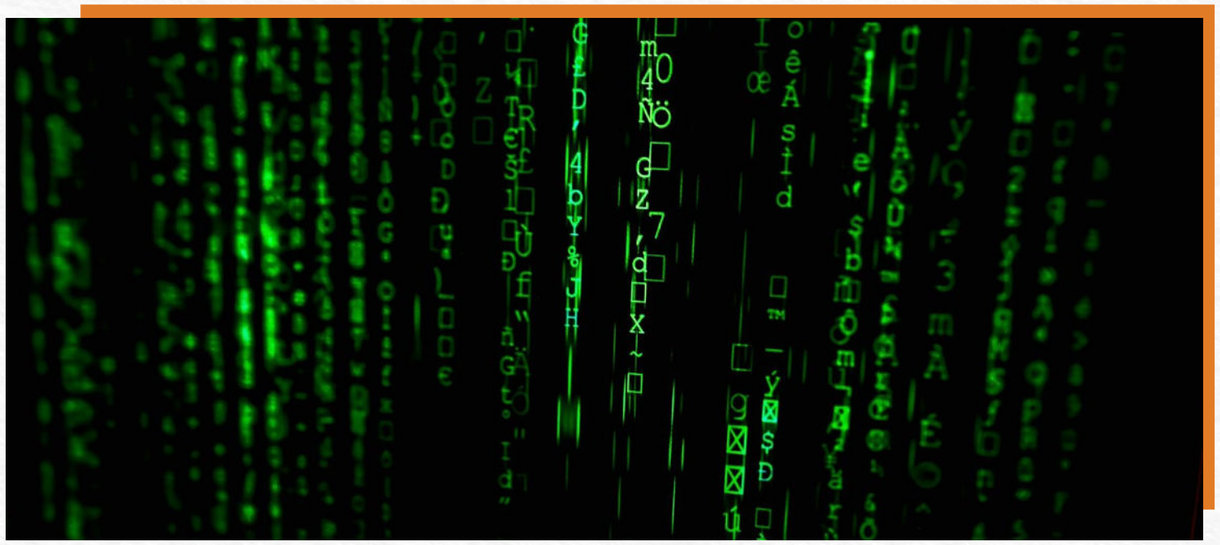
“We’re only halfway into the year, but the number of ransomware attacks has already doubled, signifying that these attacks remain effective and profitable enough for cybercriminals to ramp up their efforts,” says Vakaris Noreika, a cybersecurity expert at NordStellar.

“Some factors that could contribute to the growth in ransomware attacks include the rise in ransomware-as-a-service (RaaS), expanded attack surfaces from remote or hybrid work models, and economic uncertainty that could encourage more people to seek illegal income and turn to cybercrime.”

MAIN TARGETS IN 2025 Q2

In April-June 2025, 1,758 ransomware cases were exposed on the dark web, a 19% increase compared to the same period in 2024 (1,483 cases). Of the 1,205 ransomware incidents traced to specific victim countries, US businesses took the most brutal hit, accounting for 49% of cases (596 incidents). Germany holds the second spot with 84 cases, followed by Canada (74), the United Kingdom (40), and Spain (37).





“Not only is the US home to many profitable businesses, but the companies also have a higher profile. As a result, they’re more likely to give into ransomware demands to reduce the impact of the reputational damage resulting from an attack”, says Noreika. “Strict regulations are also a significant factor to consider — laws on data protection and operational uptime can urge companies to resolve ransomware incidents quickly and not risk the fines or loss of their clients and partners’ trust.”

Ransomware data from April to June 2025 revealed that the manufacturing industry was most affected, with 229 recorded cases. The construction industry came in second with 97 cases, followed closely by information technology (88 incidents).

The data also revealed that small and medium-sized businesses (SMBs) were the prime target for ransomware in 2025 Q2. Organisations with 51–200 employees and revenues between $5 million and $25 million faced the most ransomware attacks.

“The victim profile mirrors the data from 2025 Q1 – SMBs and companies in the manufacturing industry remain the prime targets. This is a significant cause for concern because bad actors continue successfully exploiting preventable security vulnerabilities,” says Noreika.

He explains that companies in the manufacturing industry face challenges enforcing and centralising security across all geographically dispersed locations and often rely on outdated and unpatched systems. SMBs, like manufacturing companies, often rely on third-party IT providers and lack comprehensive cybersecurity measures due to limited budgets, exposing them to greater risk.

To minimise the impact of a potential ransomware incident, Noreika recommends that businesses stay two steps ahead, implement recovery plans, and always back up critical data.

http://nordstellar.com

IPP: IOT AND AI WILL BE “GAMECHANGER” FOR INDUSTRY

Leading European pallet pooler IPP is looking ahead to the ‘game-changing’ role it believes the combination of the Internet of Things (IoT) and AI will play for the remainder of 2025 and beyond.

Stefan Herbergs, European business development director for IPP’s parent company Faber Group, said businesses were continuing to seek greater transparency, efficiency and sustainability in their operations – and that cutting-edge IoT technology was enabling IPP to respond.

Stefan said: “IoT technology is enabling us to respond to businesses’ needs with new datasets and more reliable data, ensuring end-to-end visibility across supply chains.

“IoT combined with AI will keep changing the game by offering real-time data monitoring and predictive analytics to improve efficiency.

“With IoT devices like GPS trackers, low power trackers and smart sensors, companies can better manage inventory and shipments, especially for product flows with high volume or sensitive items like pharmaceuticals.”

Stefan said that IPP was making use of AI to support and enable skilled members of its team to make smarter decisions, based on the data gathered.

While AI offers the potential for evolution, Stefan said there were also potential challenges ahead for the sector as the digital supply chain continues to evolve.

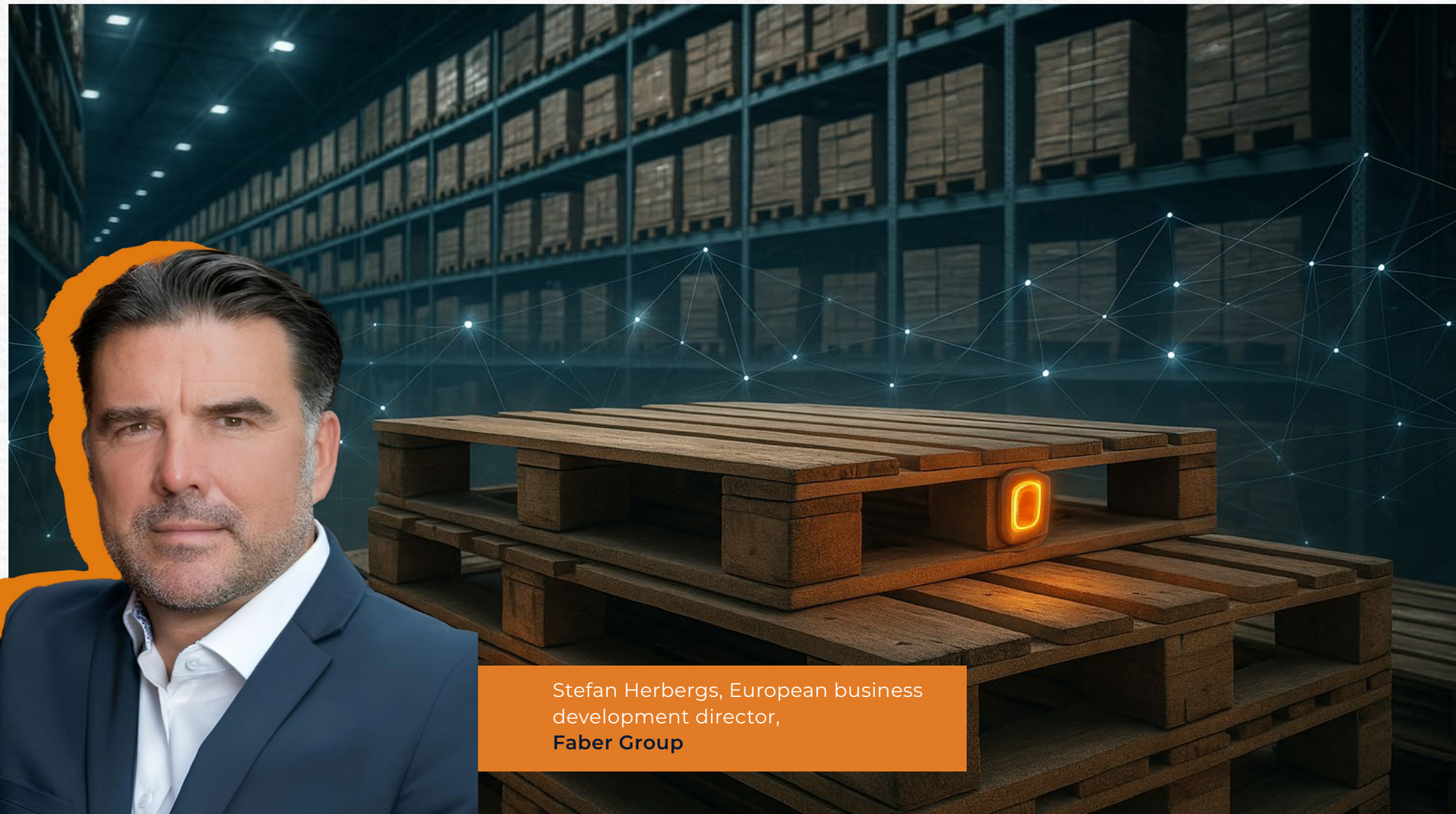
He said: “One key concern is the potential for changes in EU legislation, such as the Packaging and Packaging Waste Regulation (PPWR), which could significantly impact how companies manage recyclable materials and sustainable packaging.

“Additionally, the growing emphasis on Environmental, Social, and Governance (ESG) compliance will require businesses to demonstrate greater accountability and transparency across their operations, for instance, through the implementation of a digital product passport.”

Another potential challenge is the EU Deforestation Regulation (EUDR), which could impose stricter requirements on supply chain traceability to prevent deforestation-related activities, he added.

Stefan said: “Adapting to these regulations while maintaining efficiency, reusability, and sustainability in supply chain processes will be crucial for companies moving forward.”

www.ipp-pooling.com



Stefan Herbergs, European business development director,
Faber Group

PROACTIVELY PREPARING PHARMA FOR THE 2030 GREEN SUPPLY CHAIN

By Niklas Adamsson, Chief Operations Officer at Envirotainer

The pharmaceutical industry is at a pivotal point as we approach the 2030 deadline for achieving the UN's Sustainable Development Goals, designed to reduce emissions and take urgent action on climate change.

Rising environmental pressures, coming from both governments and consumers alike, are driving pharma companies to accelerate technological adoption to transform operations and meet stringent emissions regulations. In fact, as of 2025, pharmaceutical companies are now investing $5.2bn annually in environmental programs to transform operations, reduce waste, and introduce innovative new technologies – a 300% increase from 2020.

With sustainability a non-negotiable, pharmaceutical companies must act now to meet the 2030 deadline. Supply chains and logistics must be a significant focus for this action. With one of the biggest contributors to the industry's emission being transportation, and varying packaging, shipments and disruptions adding additional complexity to the journey, changes across the entire supply chain must be implemented effectively.

This then begs the question: how can the industry accomplish this, without impacting operational efficiency?

HOW THE PHARMACEUTICAL INDUSTRY IS SHAPING UP

The pharmaceutical industry currently accounts for almost 5% of the world's total greenhouse gas emissions. The most significant contributor to this is Scope 3 (indirect) emissions, which account for 80-90% of the sector's total climate impact. Whilst several pharma companies have focused on initiatives to reduce Scope 1 and Scope 2 emissions, Scope 3 remains difficult to target. This is largely due to the multitude of sources of these emissions, which can come from drug manufacturers, raw material producers, transporters and even the patients using the medicines or vaccines.

With green agendas front of mind, stakeholders within the pharmaceutical cold chain are introducing new initiatives, technologies, and infrastructure to ensure they can meet the 2030 deadline. Planning for this has required precision to make sure any green initiatives do not impact the efficiency or reliability of the delivery of life-saving pharmaceuticals.

A key way of addressing sustainability goals in logistics is through the choice of packaging. There are several considerations including the quantity of vaccines and medicines, the pharmaceutical's temperature requirements, autonomy required, the varying climates along the journey, and the infrastructure available on the journey and at the destination.

One option that has been gaining momentum in recent years is forever-use packaging. Engineered for reliability, longevity, and sustainability, forever-use packaging is repairable and built with high-grade materials that withstand extreme conditions. These qualities extend their lifespan significantly, helping reduce waste. Despite having a higher upfront cost, their durability makes them a cost-effective and sustainable solution in the long run.

However, in some instances forever-use packaging isn't the best option. With the need to balance reliable and efficient delivery with sustainability, single-use packaging remains the most practical solution in less developed regions which often have more dated infrastructure and face more regular supply chain disruptions. The continued innovation and diversification of packaging options remains essential, to provide a perfect solution for any given scenario.

INTEGRATING SUSTAINABILITY

Technological innovation is playing a significant part in helping providers effectively balance sustainability and efficiency in ever-changing supply chains. One of the most promising innovations in recent years has been AI. AI-driven insights can help providers determine which packaging is the most cost-effective and sustainable option by considering all the variables, including temperature requirements, climates, and available infrastructure.

By providing the technology with real-time data on transportation conditions, such as weather patterns, temperature fluctuations and route conditions, it can also determine the most sustainable and efficient route and mode of transport. Finally, the technology can also support with predicting demand, minimising overall waste of pharmaceuticals and other supplies.

Optimising routes and packaging solutions is a vital first step. However, production waste reduction strategies and a circular economy approach must be implemented across the entire supply chain to ensure the minimisation of the industry's environmental impact. Shipment monitoring technology can support with production waste reduction by enabling logistic providers to track medicines and vaccines journeys, with live updates regarding temperature fluctuations and delays. If either route or temperature has deviated, the providers can intervene immediately to reduce the likelihood of waste.

Additionally, embracing circular economy principles can revolutionise how medicines are developed, manufactured, and distributed, making it a powerful tool in the fight against Scope 3 emissions.

Niklas Adamsson, Chief Operations Officer, **Envirotainer**

Embracing change, both big and small, across the supply chain can have a significant impact to Scope 3 reductions. In fact, Envirotainer has successfully reduced its Scope 3 emissions by almost 12% in just one year, driven primarily by reduced material usage. Other contributors to this reduction are decreased weights of solutions, increased use of sea freight and the adoption of sustainable aviation fuel.

Another way to take decisive climate action is by making sustainability a critical factor when selecting suppliers and partners. By forming partnerships that further drive green initiatives forward, supply chain emissions can be effectively reduced through collaboration. Selecting the right suppliers requires attention to several factors, such as environmental capabilities, efficiency, and total life cycle waste. Building long-term partnerships will add value, not only from an environmental compliance standpoint, but also for the stability and long-term savings it can provide.

The pharmaceutical industry has made massive strides in recent years to reduce its impact on the environment ahead of the 2030 deadline. However, with five years left to build a green supply chain, additional effort is required to lessen the industry's contribution to global emissions.

Success will be achieved through collaboration across the entire supply chain, especially when it comes to Scope 3 emissions. With innovations to routes, packaging and infrastructure, the industry is now finding sustainability and operational excellence inseparable benefits of these changes. As stakeholders and consumers across the globe continue to become increasingly environmentally conscious, those in the pharmaceutical industry must continue to push for comprehensive transformation, rather than incremental changes to ensure the success of the 2030 green supply chain.

With five years to go, the industry must persevere to ensure the delivery of better outcomes for patients, businesses, and the planet.

www.envirotainer.com/

TIGHTENING PHARMA HYGIENE TO CUT CONTAMINATION RISK

By Jon Hughes, Editor

Stricter hygienic standards are reshaping pharmaceutical manufacturing. Regulators in Europe and the US have placed contamination control at the centre of sterile production, forcing companies to rethink not just how cleanrooms are operated but how equipment itself is designed. With recalls costing manufacturers tens of millions of dollars, the stakes for getting it wrong have never been higher.

The 2023 revision of EU GMP Annex 1 marked the biggest regulatory change in sterile manufacturing for a generation. The update requires every plant to adopt a Contamination Control Strategy — a live, facility-wide framework that maps every contamination risk and sets out how it is controlled. The shift is away from box-ticking and towards a science-driven, risk-based approach aligned with modern quality principles. Meanwhile, the FDA continues to emphasise Quality by Design, cleanroom design, and continuous monitoring, bringing its own flavour of regulatory rigour to the same end goal: fewer contaminants in sterile drugs.

For manufacturers, compliance is not optional, and the economics are brutal. The sterile injectables market alone is projected to reach $293 billion by 2032. In biologics and advanced therapies, single contaminated batches can wipe out months of production.

Recent recalls highlight the danger. DermaRite had to pull multiple over-the-counter products in 2025 due to Burkholderia cepacia contamination, while Amneal withdrew antibiotic tablets after microbial contamination was detected. The average pharmaceutical recall costs between $10 million and $100 million, and catastrophic cases can run far higher. These events underline why regulators are tightening the screws and why manufacturers are scrutinising every process step.

FROM OPERATOR RISK TO EQUIPMENT DESIGN

Historically, contamination control focused on operator training and gowning. Human presence remains the single largest contamination source, but the industry is now redesigning equipment and processes to minimise intervention altogether. Annex 1 sets out expectations for isolators and Restricted Access Barrier Systems, while the FDA encourages facility layouts that eliminate cross-contamination pathways.

The philosophy is the same: prevent risk at the design stage, not after the fact.

That thinking extends deep into plant equipment. Pumps, valves, and mixers are now engineered to be crevice-free, self-draining, and resistant to aggressive cleaning agents. The ASME-BPE standard sets tighter tolerances than food-grade equivalents, demanding ultra-polished surfaces and defect-free welds. These mechanical details, once seen as marginal, now sit at the heart of compliance.

It is at this level that suppliers are adjusting. Wangen Pumps, for example, recently redesigned its Twin NG hygienic pump to eliminate potential contamination traps and simplify cleaning. The addition of lantern couplings reduces stress points while hygienic machine feet allow easier wash-down and better drainage. Though a relatively small design change, it reflects a sector-wide shift: suppliers are rebuilding familiar equipment to meet the higher hygienic bar now expected in pharma, as well as in food and cosmetics.

Yet hygienic design alone does not solve the problem. Cleaning validation remains one of the heaviest operational burdens in sterile facilities, consuming up to 30% of planned production time in some operations. Failures are costly in both time and compliance risk — the FDA issued dozens of warning letters in 2022 for deficiencies in validation.

Here too, technology is stepping in. Clean-in-Place and Sterilise-in-Place systems are increasingly sensor-driven, monitoring conductivity, turbidity, and flow rates to ensure rinses finish exactly when residues are gone.

Automated logging produces the audit trails regulators expect, and optimisation reduces the chemicals and water consumed per cycle. For companies facing both sustainability targets and tightening Annex 1 expectations, this dual benefit is significant.

At the same time, pharma faces a chronic shortage of skilled aseptic operators. This is accelerating the adoption of robotics and digital oversight. Robots are now performing cleanroom material transfers and assembly tasks with a consistency no human can match — and without generating particles. Smart monitoring systems track particle counts, air pressure, and humidity in real time, flagging deviations before they threaten production. Digital twins take the concept further, simulating changes to equipment layouts or airflow patterns without disrupting live operations.

THE STERILE FRONTIER AHEAD

These shifts are not without their own contradictions. Single-use systems, now widely adopted to reduce cleaning and cross-contamination risks, also generate large volumes of plastic waste. CIP optimisation saves energy and water, yet it demands more sensors, software, and complexity. Regulators have not yet resolved these tensions, and industry will continue to balance hygiene with sustainability, efficiency, and cost.

What is clear is that contamination control is no longer just about operators in gowns or surface wipe-downs. It is embedded in equipment, coded into digital systems, and enforced by regulation that demands scientific justification at every step. The redesign of a pump, the configuration of a valve, or the addition of a monitoring sensor are all part of the same industrial movement.

As the regulatory bar rises, the pharmaceutical sector has little choice but to adapt. Equipment suppliers that can prove hygiene, compliance, and reliability in one package will shape the next generation of sterile facilities. For an industry where the cost of a single contamination event can dwarf the investment required to prevent it, the calculus is increasingly obvious.

IN CONVERSATION DAEL WILLIAMSON, DATABRICKS

In your experience, how are industrial manufacturers redefining supply chain resilience in the AI era?

"Traditionally, supply chain resilience was synonymous with buffer inventory, contingency stockpiles, and back-up logistics. However, that model is becoming obsolete. Manufacturers are re-architecting their supply chains to be intelligent, adaptive, and driven by real-time data.

"AI plays a central role in this evolution. Instead of reacting to disruptions after the fact, manufacturers are now using predictive analytics to forecast demand shifts, spot supplier risks and model potential outcomes. This proactive approach minimises downtime and helps manufacturers get ahead of problems before they even occur.

"Another key change is the drive towards unified data environments. Manufacturers are integrating information across ERP systems, logistics platforms and IoT devices to get a single, real-time view of their operations. This end-to-end visibility, powered by AI, makes it easier to detect bottlenecks and optimise performance on the fly.

"Essentially, AI is shifting the paradigm of supply chain resilience from reactive to proactive, allowing businesses to predict challenges and stay one step ahead."

You've emphasised the importance of treating supplier networks as strategic assets. Could you elaborate on how AI and data infrastructure support this shift? What practical steps can companies take to transform their supplier relationships through AI?

"Supplier networks have become a vital source of competitive advantage - especially when supported by real-time data sharing and AI-driven collaboration. To move beyond transactional relationships, companies need to integrate systems and processes with their partners, creating shared visibility across forecasting, inventory, and logistics.

"This collaborative environment allows for everyone to work together on tasks like joint forecasting, inventory control and risk assessment. It also enhances the responsiveness between parties and aligns on company goals. So, to put this into practice, businesses should invest in interoperable data platforms that facilitate smooth integration with supplier systems. Having standardised data protocols guarantees uniformity and promotes clear communication.

"Additionally, implementing AI-powered supplier performance monitoring tools helps pinpoint areas in need of innovation and development. When manufacturers and suppliers work together, sharing ideas and solving problems as a team, it opens the door for continuous improvement and real value creation on both sides."

Data fragmentation is a common challenge in industrial supply chains. How can organisations overcome this to enable AI-driven insights across their networks? What role does interoperability play in this context?

"Fragmented data environments create blind spots that limit the effectiveness of AI. When information is scattered across incompatible systems, it's nearly impossible to generate reliable, real-time insights. To overcome this challenge, organisations must prioritise data integration and interoperability as a foundational principle of their digital strategy.

"Implementing standardised data platforms, such as data lakes, which combine several data sources into a single, cohesive environment, is a powerful way to achieve this. Due to this interoperable standardisation, AI-driven analytics can produce thorough insights and facilitate enhanced strategic decision-making.

"Interoperability is essential in this transformation. Organisations can guarantee seamless communication between various systems and stakeholders by adopting open data standards and APIs. Throughout the supply chain, this connectivity improves responsiveness and collaboration by facilitating real-time data transmission.

DAEL WILLIAMSON, EMEA CTO, **DATABRICKS**

"Reliable AI results also depend on data security, compliance, and quality, all of which are guaranteed by investing in data governance systems. By tackling data fragmentation through interoperability and integration, businesses can fully unlock the potential of AI and increase supply chain resilience and efficiency."

Can you share examples of how companies are using AI to respond dynamically to disruptions such as raw material shortages or logistics delays?

"AI is playing a critical role in helping companies adapt quickly to growing supply chain disruptions. For instance, when faced with raw material shortages, businesses are using predictive analytics to process signals from supplier data, market trends and geopolitical developments. This allows them to anticipate risks early and take action - whether by securing alternative suppliers, adjusting order volumes, or rebalancing production schedules.

"In logistics, AI is helping companies respond to real-time conditions by optimising delivery routes based on traffic patterns, weather forecasts and transportation availability. Despite disruptions, its dynamic routing reduces delays and guarantees on-time delivery. Digital twins driven by AI also enable businesses to generate different disruption scenarios and evaluate the operational impacts. When interruptions happen, these models allow for quick response and inform contingency planning."

Standards like Delta Sharing are gaining attention for enabling secure, real-time collaboration between supply partners. Why are such standards particularly important for manufacturers operating in complex ecosystems, and how do they bolster supply chain resilience?

"In complex manufacturing ecosystems, the ability to share data securely and instantly across partners is no longer a nice to have - it's essential. Standards like Delta Sharing, which offer a safe and effective framework for real-time data exchange, facilitate this smooth data transmission, enhancing supply chain resilience. Real-time access to interoperable, shared data improves supply chain visibility, enabling coordinated operations and quick reaction to interruptions or changes.

"On top of this, regulated data sharing strengthens collaborative relationships by promoting transparency and trust among partners. When partners know the data is accurate, secure and controlled, it becomes far easier to work together on strategic planning and contingency response. That transparency turns fragmented supplier relationships into resilient, high-performing networks."

For operations leaders in traditional industries who are hesitant about adopting AI, what would you advise as the first steps toward building a smarter, more resilient supply chain?

"Adopting AI doesn't require a wholesale transformation from day one. Small, focused efforts at first, nevertheless, can show value and inspire confidence. Start by pinpointing certain supply chain problems, such as demand forecasting for inventory management, where AI might offer immediate benefits. Applying AI solutions in these fields can demonstrate the technology's potential and help you build a smarter, more resilient supply chain.

"Data infrastructure investment is also essential. Effective AI implementation is based on ensuring data integration, quality, and accessibility. Teams are also more likely to adopt new technology when an innovative and continuous learning culture is promoted. Giving staff members access to materials and training demystifies AI and enables them to take full advantage of its potential.

"Starting small, building on real wins, and enabling people through the right tools and mindset is how traditional operations can evolve into intelligent, resilient networks powered by AI."

"Starting small, building on real wins, and enabling people through the right tools and mindset is how traditional operations can evolve into intelligent, resilient networks powered by AI."

www.databricks.com/


IN
INDUSTRIAL
NEWS