VISIT REPORT

sido
16/17.09.2026
CITÉ INTERNATIONALE DE LYON

BNB markets

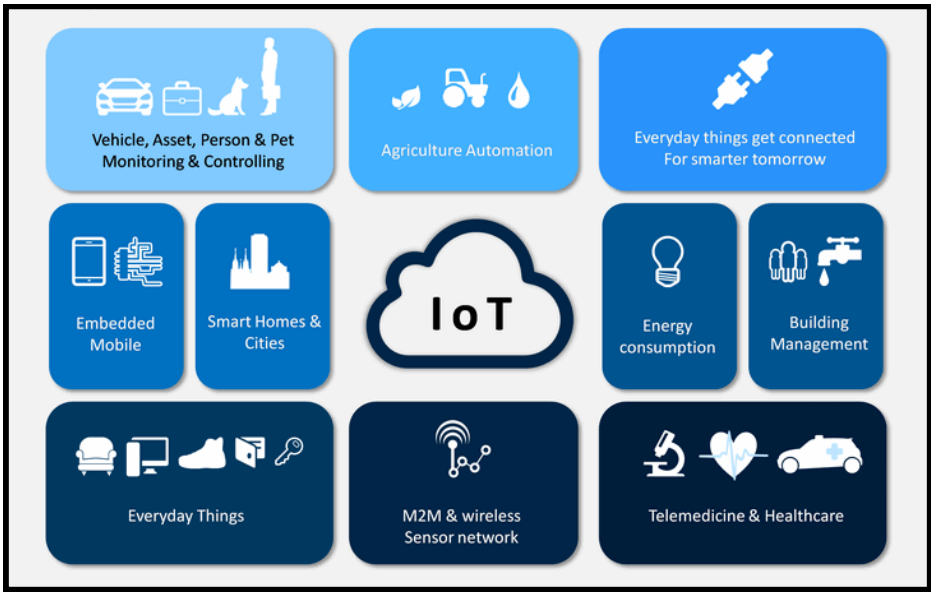


OVERALL PRESENTATION

Pioneering event in Europe on the convergence of IoT, AI, XR & Robotics technologies, SIDO[1] makes the link between technological solutions and Startups, SMEs, mid-size companies and international Groups by facilitating technological partnerships and cooperation in all sectors of activity.

Since its creation in 2015, SIDO Lyon has been the historical event for all the key players in the IoT, AI, XR & Robotics ecosystem: tech solution providers, industrial groups, research laboratories, local authorities, institutions, etc. As a key event in the decision-makers' calendar, SIDO supports companies in their digitization projects by bringing together technological leaders over a two-day trade show. For its 12th edition, held on 16–17 September 2026 at the Cité Internationale de Lyon, the show adopted a clear guiding theme: "From field data to deployable performance". From innovative bricks to complete and ready-to-go solutions, the entire value chain is represented, organized around a six-step value cycle: Measure, Analyze, Simulate, Deploy, Verify and Pilot.

Situated in the heart of Lyon and the Auvergne-Rhône-Alpes region, SIDO thrives on a diverse industrial base, including metallurgy, plastics, chemistry, electronics, pharmaceuticals, agri-food, textiles, machinery, and equipment. For more than a decade, SIDO has been an essential event for business leaders, strategic decision-makers, innovators, and managers seeking long-term growth and value creation. Decision-makers account for 62% of its visitors, and in 2025, 69% of visitors came from Auvergne-Rhône-Alpes and 60% from B2B industries.



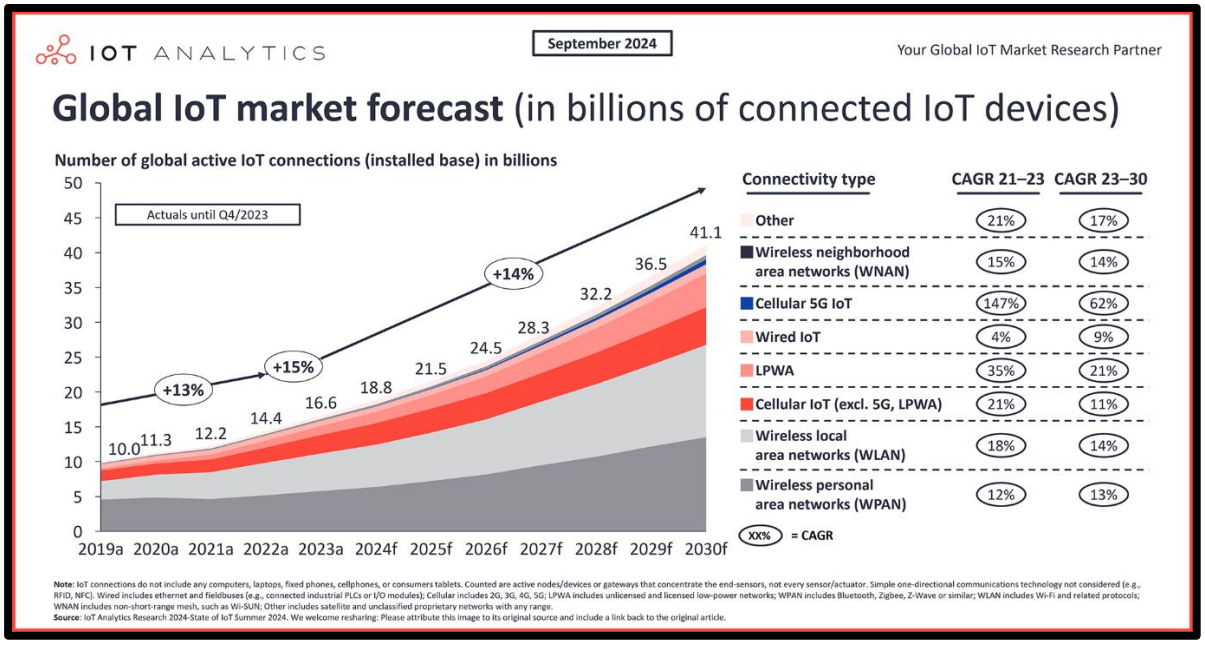
[1] SIDO (for "Solution Internet des Objets") is a trade show organized by Infopro Digital Trade Shows, a subsidiary of Infopro Digital group, which is a world leader in information and services for professionals. The show focuses on IoT, AI, Robotics and XR solutions and technologies. It takes place at the Cité Internationale de Lyon and is considered the largest European showroom for these technologies. Through thematic routes which will facilitate professional visits, it offers around 70 conferences or workshops which will allow key subjects of the digital transformation (innovation strategy, process optimization, system interoperability, etc.). Some 300 exhibitors and nearly 8,000 visitors attend, from most of the French blue chips companies. Thus, innovative companies, start-ups, manufacturers and other suppliers of cutting-edge technologies for the Internet of Things, AI and robotics gather around numerous exhibitors presenting their products and services working for an effective digital transition.

© BLACKNBLUE MARKETS 2026

The Internet of Things (IoT) is a term used to describe the growing network of interconnected devices that we interact with in our daily lives. As the Internet expanded, telephones, office equipment like printers and scanners, and industrial machines were integrated into the network. Today, almost any device we use, whether at home, in the office, or on the go, can be connected to the Internet. This has given rise to the concept of the Internet of "Things". The IoT encompasses a wide range of devices and technologies that enable seamless communication and data exchange between physical objects and digital systems. The IoT is a trend that is driving the digitization and datafication of society in many new and exciting ways. Connected devices such as autonomous cars, everyday objects, autonomous manufacturing robots, and remote medical devices that enable doctors to diagnose patients and even perform surgical procedures are all made possible by these networks of connected objects.

In 2025, cyberattacks reached record levels. According to Check Point's Cyber Security Report 2026 (January 2026), organizations faced an average of 1,968 cyberattacks per week, a 70% increase since 2023. Ransomware has fragmented into smaller, specialized groups, with a 53% year-over-year increase in extorted victims and a 50% rise in new ransomware-as-a-service groups. Unmonitored edge devices, VPN appliances and IoT systems are increasingly used as stealthy entry points and relays. AI itself has become an attack surface: 89% of organizations encountered risky AI prompts over a three-month period, and security weaknesses were found in 40% of 10,000 Model Context Protocol (MCP) servers reviewed. On the regulatory side, the EU Cyber Resilience Act requires manufacturers to report actively exploited vulnerabilities in connected products from 11 September 2026, a few days before the show. It is easy to understand why SIDO, for its 12th edition, once again hosts the Lyon Cyber Expo to better address the growing threat landscape and emphasize the importance of robust cybersecurity measures.

Number of connected IoT devices to grow 14% to 21.1 billion in 2025. According to IoT Analytics (State of IoT, October 2025), there were 18.5 billion connected IoT devices at the end of 2024 (a growth of 12% over 2023). IoT Analytics expected this to grow 14% to 21.1 billion by the end of 2025, and forecasts 39 billion connected devices in 2030 and more than 50 billion by 2035, with AI as a key growth driver.



As L'Usine Nouvelle rightly noted a few years ago, SIDO is an exhibition dedicated to robotics, artificial intelligence, and the Internet of Things. This event is less about closing contracts and more about

© BLACKNBLUE MARKETS 2026

staying informed and gaining visibility. For the third year in a row, the show is co-located with the Lyon Cyber Expo, offering a space dedicated to the protection of digital infrastructures. 2026 is also the last edition at the Cité Internationale: in September 2027, SIDO moves to Eurexpo Lyon.

I suggest you take an overview of the show through this brief report. After some insights and descriptions of the AI market, you will find a list of the conferences and presentations, each accompanied by an extract from the program and the topics covered. For some, I've included personal remarks written after attending the sessions.

MARKET TRENDS WITH AI

The global artificial intelligence (AI) market continues its rapid expansion. Valued at $391 billion in 2025, it is estimated at **$539.5 billion in 2026, with a projected compound annual growth rate (CAGR) of 30.6% through 2033**, when it could reach nearly $3.5 trillion (Grand View Research). This momentum is driven by the enterprise adoption of generative and agentic AI, investment in AI infrastructure and chips, and the maturation of AI technologies.

AI is transitioning from experimental applications to operational deployment, becoming a core enabler of real-time personalization, automation, and advanced analytics. According to the Stanford AI Index 2026, 88% of surveyed organizations used AI in 2025 and 70% used generative AI in at least one business function, with China and Europe posting the strongest year-over-year increases. In the European Union, 20% of enterprises with 10 or more employees used AI in 2025, up from 13.5% in 2024 (Eurostat). Sectors such as retail, healthcare, and manufacturing are increasingly integrating AI to enhance efficiency, customer experience, and decision-making capabilities.

Several emerging trends are shaping the future of AI. Agentic AI, systems capable of more autonomous decision-making, is the trend of the year: Gartner expects 40% of enterprise applications to embed task-specific AI agents by the end of 2026, up from less than 5% in 2025. Actual deployment, however, remains in the single digits across most business functions (Stanford AI Index 2026). Edge AI, which enables local processing on sensors, machines and IoT systems for improved speed and data security, is also gaining ground, together with energy-efficient models. **Additionally, the development of specialized small models is addressing the needs of resource-constrained environments, making AI more accessible and adaptable.**

In the workforce, AI adoption is accelerating at an impressive pace. AI skills now appear in 2.5% of all US job postings, up 55% in one year, and demand for agentic AI skills nearly quadrupled in 2025 (Stanford AI Index 2026, Lightcast data). However, this surge is also creating disparities: in Europe, 55% of large enterprises use AI against only 19% of SMEs (Eurostat), and smaller entities often struggle to keep up with the pace of innovation. AI's influence on the job market is multifaceted. It is simultaneously displacing certain roles and generating new opportunities, particularly in cutting-edge fields such as drug development and autonomous vehicles. As AI continues to evolve, its impact will be felt across both economic structures and societal norms.

© BLACKNBLUE MARKETS 2026

SIDO LYON 2026 HIGHLIGHTS

The 12th SIDO Lyon, held on 16–17 September 2026 at the Cité Internationale (Lyon Convention Centre), confirmed its status as a premier European gathering for professionals in IoT, AI, XR, and robotics. With nearly 8,000 professional visitors and 300 exhibitors, the event showcased the vibrancy and innovation driving the tech ecosystem.

Some 70 conferences, round tables and workshops, with around 200 announced speakers, addressed pivotal themes such as industrial IoT, edge computing, generative and agentic AI, digital twins, robotics and cobotics, AMRs, and integration with MES, ERP and CMMS software. Formats ranged from plenary sessions on technological and geopolitical issues to "100% end-user" experience-sharing sessions. Speakers included representatives of France 2030, CNRS, Crédit Agricole and the AI, Data & Robotics Association, as well as Hervé Groléas (Métropole de Lyon), Laurence Lacombe (CIO, LDLC), Fayçal Rezgui (CEO, Araïko) and Frédéric Hélin (Coboteam cluster).

A key highlight of the 2026 edition was the shift from proof of concept to deployment. As Yannick Villain, Director of SIDO Lyon, put it: "We are no longer talking about trends or technological promises; we are talking about deployed solutions, concrete feedback and measurable results." The co-located Lyon Cyber Expo (3rd edition, 160 solution providers) reinforced this message: every newly connected machine or automated line is also a potential entry point into the information system.

New and returning features included INNOROBO, a space dedicated to deployable robotics in synergy with AI (productivity, labor shortages, reindustrialization); IMPACT by SIDO, back for a third time, focused on responsible digital technology; an expanded Start-up Village; and an appointment-booking app. On the exhibitor side, edge AI and secure connectivity were everywhere: STMicroelectronics showcased edge AI, connectivity and sensing; IXON presented SecureEdge, an IEC 62443-4-2 certified gateway; Steliau Technology unveiled the ANNA-B5 Bluetooth Low Energy module; and the LoRa Alliance highlighted LoRaWAN, which connects more than 125 million devices worldwide. Lyon Cyber Expo, organized around strategy and preparation, protection and detection, and crisis management, focused on NIS2, IEC 62443 and the Cyber Resilience Act.

SIDO Lyon continues to be a catalyst for cross-sector collaboration, encouraging companies to identify and adopt transformative technologies. Its influence is particularly strong in manufacturing, logistics, and public sector services, where innovation is reshaping traditional models and unlocking new opportunities. Next step: the 13th edition will take place on 15–16 September 2027 at Eurexpo Lyon, alongside 3D PRINT Congress & Exhibition and INNOROBO, to create a major event dedicated to new technologies and industrial transformation.

> AI has moved from experimentation to deployment, as illustrated by SIDO Lyon 2026. French and European industry are now focusing on measurable, secure and sovereign integration of AI, from field data to production lines and leverage events like SIDO to network, benchmark, and drive innovation.

These trends indicate that AI is no longer an isolated technology but a foundational layer for industrial and digital strategies, with events like SIDO Lyon serving as important barometers of progress and collaboration in the field.

© BLACKNBLUE MARKETS 2026

CONFERENCE AND BUSINESS PRESENTATIONS WEDNESDAY SEPT.16

Analytical, generative, agent-based: when AI boosts robots' autonomy

Alain Bensoussan, Lexing Avocats
Fabrice Deblock
Frédéric Hélin, Coboteam Auvergne-Rhône-Alpes
Fabrice Jumel, CPE Lyon

Industrial robots have long been programmed to repeat specific tasks in controlled environments. But with the advent of new forms of artificial intelligence – analytical, generative and now agent-based – a new generation of robots is emerging, capable of adapting, planning, understanding their environment and making certain decisions autonomously. Analytical AI enables the use of sensor data to optimise trajectories, maintenance or quality. Generative AI paves the way for programming in natural language, simulation and the learning of new tasks. Finally, agentic AI enables the orchestration of actions, collaboration with other machines and real-time adaptation to production contingencies. But how far can we go in terms of robot autonomy? Which tasks can actually be automated today? What are the technological barriers, and the challenges regarding safety, cybersecurity and liability? And how can these new capabilities be integrated into existing industrial environments?

Innovating in a constrained world: the end of technological abundance?

Frédéric Bordage, Green IT
Julia Delrieu, Digital League
Erwann Fangeat, ADEME
Gillo Malpart, Mavana.earth
Tristan Nitot, Octo Technology

For years, digital innovation has been underpinned by a sense of abundance: accessible computing power, virtually unlimited storage, readily available components, relatively cheap energy, and the proliferation of cloud services. This model has enabled an unprecedented acceleration of technological projects, from the Internet of Things to artificial intelligence. But the landscape is changing rapidly. Rising energy costs, pressure on resources, environmental constraints, technological dependencies, regulatory pressure, a shortage of certain skills… Companies must now navigate a more constrained environment, where every technological choice has economic, environmental and strategic implications. Should we continue to innovate at the same pace, or fundamentally rethink how we design digital systems? How do we balance performance, efficiency, security and costs? Will innovation come through more frugal technologies, optimised architectures and better use of existing resources?

BNB markets. *The era of technological abundance is ending. Cheap energy, available metals and components and almost unlimited computing power can no longer be taken for granted. Innovation now has to work within constraints: design for real needs, make existing hardware last longer and stay in control of our tools, including AI. Erwann Fangeat (ADEME) opened with the figures. Digital technology could account for more than half of per-capita CO2 emissions in the coming years. In France, it currently uses 46 TWh of electricity or 65 TWh including data centers abroad. This could reach about 100 TWh by 2050, and up to 300 TWh including foreign data centers. ADEME's own projections are similar: more than 250 TWh a year for French digital use by 2050, foreign data centers included.*

© BLACKNBLUE MARKETS 2026

According to an IRIS study, the main bottleneck for AI deployment by US big tech is access to the power grid. Resources are a concern too: a smartphone contains around 50 metals and China is the top producer of 25 metals and the only producer of 7.

Sometimes digital can simply be removed: farmers need a text message for rainfall data, not a 4G smartphone. He calls this new approach slow tech: keep high tech only where it is essential and use low tech everywhere else. Constraints can drive innovation rather than hold it back. The main levers are eco-design, longer hardware life, low tech or slow tech where possible and leaner software. AI should be used with judgment, so it does not erode our skills. Control over metals, open source and data centers, along with training, is becoming a strategic issue for companies.

SGP.32: From Hype to Business Value, making your IoT connectivity evolve without adding unnecessary complexity

Marco Corona, Wireless Logic

You have connected devices deployed in the field, and one day your connectivity will need to evolve: switching supplier, entering a new market, or simply no longer depending on a single operator. SGP.32 makes this possible. But to get the most out of it, everything comes down to choosing the right operating model and the right partners for your specific business needs. This workshop gives you a straight answer on: where the eSIM market really stands today, the technical challenges to anticipate and the value SGP.32 delivers in practice for businesses, why there's no universal eSIM strategy and which criteria determine the right choice for each business, why the value of SGP.32 depends as much on your business objectives as on choosing the right partners. You'll walk away with a precise understanding of the business value SGP.32 can create for your company, and the criteria to choose the deployment model that fits your needs.

Smart City, Smart Building, Industry: Supervisor vs Hypervisor – the battle of the IoT platforms

Philippe Combey, Auxilium Strategicum
Steven Dolbeau, Anima Conseil
Dominique Legrand, AN2V
Yvan Ridé, Cthings

IoT platforms are proliferating across all sectors: industry, smart buildings, smart cities, energy, infrastructure… But behind this generic term lie very different realities: monitoring platforms, hypervision platforms, data platforms, cloud-based IoT platforms, and multi-system integration platforms. The result: businesses and local authorities are faced with a multitude of possible offerings and architectures, with a risk of technological dependency and the proliferation of silos. Is a single platform capable of supervising everything required? What is the difference between supervision and hypervision? Where should the platform be located: on-premises, in the cloud, or at the edge? How can heterogeneous systems be integrated: building management systems, industrial automation, IoT sensors, energy systems, security, maintenance, and data platforms? And above all, how can we avoid creating new digital silos under the guise of a single platform?

© BLACKNBLUE MARKETS 2026

Ensuring the security of all uses of AI, without stifling innovation

Olivier Vaugrenard, Netmetrix

AI has become an essential and indispensable tool for business operations. Its widespread adoption across finance, legal, marketing, human resources, development teams and other areas adds value, but also introduces new challenges and risks that are critical to corporate security. Identifying hidden AI uses within the organisation, detecting risky behaviour in real time, limiting leaks of sensitive data, and providing visibility and governance over the AI tools in use: managing these risks means protecting the organisation's data, its reputation and its regulatory compliance. This workshop will show you how to secure all these applications, whilst allowing teams to continue innovating with AI without hindering their productivity.

Plenary Session, Wednesday Morning

Digital sovereignty cannot be imposed; it must be built

Julien Bergounhoux, L'Usine Digitale
Jean-Noël de Galzain, Wallix / Hexatrust
Florent Kirchner, Secrétariat Général pour l'Investissement / France 2030
Christophe Leray, STEF
Christophe Lombard, CANUT

In the face of growing dependence on foreign technologies – cloud services, software, components and artificial intelligence – digital sovereignty is emerging as a key strategic issue for both businesses and governments. Yet, between political announcements and declarations of intent from major corporations, digital sovereignty is still too often the subject of empty rhetoric rather than operational reality. Today, voices are being raised to put forward a pragmatic vision of the issue, with an industrial and economic perspective: digital sovereignty cannot be decreed; it must be built and measured. Whilst French and European solutions do exist, driven by players who sometimes sell better internationally than in their domestic market, the issue of public and private procurement – that of the state and large corporations which, through their purchasing volumes, shape the market – becomes critical. The same applies to the issue of funding, which, whilst effective for start-up funding, falls short when it comes to scaling up – a crucial stage in preventing European companies from seeking funding elsewhere, selling out or relocating. So, can we finally build a digital sovereignty that stands on its own two feet? Here are some answers.

BNB markets. *Digital sovereignty is a matter of state policy but for companies the real issue is digital resilience. No business can run without IT and a cloud or SaaS provider can shut down a service with one click. A few dominant giants impose their terms and geopolitics adds risk because one leader's unilateral decision can cut off access. Being resilient means being able to make your own decisions and having the means to carry them out, yet many leaders still see IT as a mere support function. French and European alternatives exist and can match the big players, but switching is hard. Jean-Noël de Galzain said buyers have to change their habits: add sovereignty to purchasing criteria, reason in total cost of ownership and build trusted solutions rather than selling fear. Public procurement is the key lever: US tech firms get 15 to 40% of their revenue from public contracts when they go public, so national preference should apply to both public and private buying. AI makes these decisions more*

© BLACKNBLUE MARKETS 2026

urgent. Christophe Lombard warned that French companies can still end up under American ownership, so each industry needs to organize, with change management and courage. The bottom line: take back control of purchasing, needs and offers instead of putting up with dependence.

State-sponsored attacks: the tactics of cynical titans

Stéphane Cozette, Hornet Security

Cyberattacks have changed significantly: they are no longer opportunistic but targeted, carried out by organised groups operating like fully-fledged businesses. Through Ransomware-as-a-Service and Phishing-as-a-Service, attackers are industrialising their campaigns and exploiting Microsoft 365 environments to compromise identities, bypass MFA, map data, move laterally and exfiltrate sensitive information. The rise of Large Language Models (LLMs) and AI agents also introduces new risks, such as prompt injection attacks, which exploit connected agents. In the face of these threats, detection alone is no longer sufficient: it is essential to automate the response, whilst strengthening user awareness and governance of messaging and collaborative working environments.

Patents and software: maximising the value of intangible assets to accelerate growth

Salomé Basset, Ayming
Guillaume Brunel, INPI
Patrice Charton, Ayming
Fabien Fabron, Mukeï

Patents, software, algorithms, know-how: assets derived from R&D now represent a strategic driver of competitiveness and growth for innovative companies. Yet their value is often under-exploited. During this workshop, we will share methods for transforming innovation into tangible economic value. Discussions will cover the various approaches to monetising intellectual property assets, the opportunities offered by the IP Box scheme, and the links between R&D investment, intellectual property strategy and financial performance. The aim of this session? To equip participants with the tools to better identify, protect, monetise and capitalise on their intangible assets in an increasingly competitive innovation landscape.

Industrial connectivity: 5G, LoRaWAN, industrial Wi-Fi, which will come out on top?

Olivier Amiot, Sequans
Jean-Philippe Chouika, Wireless Logic
Maxence Cossalter, Anima Conseil
Éric Djakam, STMicroelectronics
Matthieu Plagnol, ECAM LaSalle Lyon

Connectivity has become a critical infrastructure for industry: IoT sensors, connected machines, mobile robots, remote maintenance, augmented reality, logistics tracking, real-time data collection… But

© BLACKNBLUE MARKETS 2026

faced with a proliferation of technologies – private 5G, LoRaWAN, industrial Wi-Fi, mesh networks, edge computing – manufacturers must make strategic choices that will commit their investments for many years to come. Should a private 5G network be deployed in the factory? Is LoRaWAN sufficient for industrial sensors? Does industrial WiFi remain the simplest and most cost-effective solution? Is there a dominant technology, or should we instead learn to integrate multiple networks depending on their use? And what are the selection criteria: cost, performance, cybersecurity, energy consumption, ease of deployment, sovereignty?

***BNB markets**. No single technology wins: each one fits a use case, and the real challenge is combining them. Mathieu Plagnol explained that LoRaWAN carries small amounts of data in harsh outdoor settings, such as water flow in a river or temperature in a field. Private 5G and industrial Wi-Fi handle heavier traffic, but 5G needs state approval for its frequencies, unlike the others. He recommends a mature system built on proven technology over an immature one built on the latest, with security planned across the whole network.*

Eric Djakam (STMicroelectronics) listed the selection criteria: do you master the technology, is it secure, and how much energy does it use? Products' environmental impact has to be assessed from the start. The EU Cyber Resilience Act is a key text to follow, and ST has dedicated teams working on it. ZigBee was also mentioned as an option. Olivier Amiot reminded the audience that a technology lasts about 20 years. 3G, launched in the early 2000s, is now being switched off and its frequencies reused for 5G, so check how long a standard will be supported before investing. Private 5G is costly for a factory but very flexible. 6G should be operational around 2040 and will coexist with 5G as an evolution, not a break. Jean-Philippe Chouika concluded that architecture matters more than technology. The value chain is very fragmented, so projects bring together several suppliers and depend on interoperability and security in the upper layers. The right choice is the one that meets your needs and stays open to change.

Industry, Services: Is robotics accessible to SMEs?

Sylvie Algarra, Réseau 3R
Thierry Alvergnat, Acuytiv
Grégoire de Langautier, Maison MGA
Youssef Fadoul, Auvergne-Rhône-Alpes Entreprises
Frédéric Hélin, Coboteam Auvergne-Rhône-Alpes

Long reserved for large industrial companies, robotics is gradually becoming accessible to smaller organisations, including SMEs and businesses in the service sectors: logistics, food processing, healthcare, cleaning, retail, construction, agriculture… With the falling cost of robots, the arrival of collaborative robots, AMRs, Robot-as-a-Service (RaaS) and solutions that are easier to deploy, the market appears to be reaching a tipping point. But is robotisation really accessible to SMEs? Where should they start? Which processes should be automated first? Should they invest, lease or pool resources? How can they assess the return on investment? What in-house skills are required? And what are the real barriers: financial, organisational, human or technical?

© BLACKNBLUE MARKETS 2026

New smart sensor architectures used in smart industry and agriculture applications

Zoltán Kiss, Endrich Group
Bülent Solan, Quarterwave GmbH

Smart sensor systems are moving from single connected devices towards complete, application-driven wireless IoT ecosystems. In this presentation, we will explore new smart sensor architectures for smart industry, smart city and smart agriculture, based on the Endrich E-IoT ecosystem. The focus is on wireless networking: when to use direct cellular LPWAN, when local sensor WLANs and mesh networks are the better choice, and how gateways, delayed upload, cloud dashboards and AI-supported evaluation complete the system. We are going to review the subject from a network architectural point of view as well as from an RF point of view, touching antenna design methods. Real examples will include environmental sensing, asset tracking, refrigeration monitoring and agricultural monitoring. Special attention will be given to livestock localization and activity logging, where infrastructure-free mesh networking and cloud-side intelligence create scalable, low-power solutions.

NIS2, CRA: leaders on the front line

Jean-Noël de Galzain, Wallix / Hexatrust
Alexandre Diehl, Lawint
Nicolas Dooghe, CLUSIR Auvergne-Rhône-Alpes
Marie Leynaud, Deuxième Écoute
Jean-Christophe Marpeau, Cap'tronic
Emmanuel Petit, Club 27001

With the NIS2 Directive and the Cyber Resilience Act (CRA), cybersecurity is no longer merely a technical issue: it is becoming a matter of governance and accountability at the highest level of the organisation. These new European regulations impose stricter requirements regarding cyber risk management, product security, vulnerability management, incident reporting and organisational accountability. And for the first time, senior executives may be held directly liable in the event of a breach. But what do NIS2 and the CRA actually mean for senior management? What decisions need to be taken at the level of the Executive Committee or the Board of Directors? What investments should be planned? How should cyber governance, risk management, compliance and crisis management be organised? And how can these regulatory constraints be turned into a lever for improving the company’s security and resilience?

Agriculture, logistics, security, construction, healthcare: drones are taking off

Xavier Brenière, Lynred
Antoine Level, Delair / ADIF
Jean-Philippe Malicet, Cap'Tronic
Nicolas Marchand, GIPSA-Lab

Long confined to experimental uses or aerial photography, drones are now establishing themselves as genuine operational tools across a wide range of sectors: precision farming, infrastructure inspection,

© BLACKNBLUE MARKETS 2026

surveillance of sensitive sites, construction site monitoring, logistics inventory, delivery, emergency response and applications in the healthcare sector. They hold great promise: accessing difficult-to-reach areas, reducing human risk, speeding up operations, collecting real-time data and automating certain tasks. But their large-scale deployment still raises many questions: regulatory framework, flight safety, cybersecurity, integration into business processes, data management, social acceptance and return on investment. Which use cases are actually working today? Where does the concrete value lie for businesses and local authorities? What are the technical, economic and regulatory limitations? And how can drones be integrated into existing value chains without complicating operations?

Digital trust and third-party suppliers: reducing risks without burdensome audits

Guillaume Collard, CSB School
Fabrice Didier, Dimo Software
Steven Dolbeau, Anima Conseil
Géraud Gonzalez, EY
Kevin Muller, Passbolt
Emmanuel Petit, Club 27001

Today, businesses are increasingly reliant on their digital suppliers: software publishers, system integrators, IT service providers, cloud platforms, connected devices, industrial subcontractors… This constant interconnection creates a new reality: a company's level of cybersecurity also depends on that of its partners. But for many organisations, assessing supplier security is becoming a headache: lengthy and costly audits, complex questionnaires, a lack of visibility, and difficulty in monitoring over time. How can a supplier's level of trustworthiness be assessed without deploying cumbersome and time-consuming audit processes? What practical methods can be put in place for SMEs and mid-market companies? Should assessments be standardised? Can audits be pooled? What role do certifications, labels, assessment platforms or cyber ratings play?

Industrial ETI: how adaptive defence secures your production lines

Arnaud Loubatière, SoSafe SAS

For the manufacturing sector, a cyberattack is not just an IT incident: it means the sudden shutdown of production lines and an immediate loss of revenue. With the growing convergence of IT and OT, the factory of the future is hyper-connected, making it a prime target. This 45-minute workshop, designed to address the specific challenges faced by mid-sized enterprises, offers a resolutely pragmatic approach. How can you protect an industrial environment where uptime is paramount and critical systems cannot be paused? Discover how adaptive defence is emerging as the business solution par excellence: agile security, capable of identifying threats and adapting to the constraints of the factory, to protect production facilities without ever slowing down the pace.

© BLACKNBLUE MARKETS 2026

IoT: how do you move from a proof of concept to a large-scale roll-out?

Nicolas Andriot, Vodafone
Maxence Cossalter, Anima Conseil
Philippe Flatresse, Asteerics
Julien Fournier, IT Novem (Groupe SNCF)

Many companies have already carried out IoT Proof of Concept (POC) projects: connected sensors, predictive maintenance, asset tracking, energy management, smart buildings, connected logistics… But the gap between a successful pilot and large-scale deployment is often wider than expected. Issues with industrialisation, connectivity, IT/OT integration, cybersecurity, data management, sensor maintenance, operating costs… Many projects get stuck at the experimental stage. What are the barriers preventing scaling up? Should we first focus on the platform, connectivity, data, cybersecurity and internal organisation? How can we build a viable business model? How do we manage the transition from a few dozen to several thousand connected devices? Discover how to avoid the trap of perpetual POCs and how to build a genuine, large-scale, sustainable and profitable IoT deployment strategy.

Logistics and Transport, Agriculture, Energy, Resource Management: the space IoT is spreading its wings

Didier Flaender, Flaender
David Gal-Reignez, Minalogic
Valérian Mannoni, CEA-Leti
Jonathan Miquel, Kinéis

Long reserved for scientific or military purposes, space technology is now opening up to industrial applications and everyday services. Thanks to satellite constellations, new communication capabilities and Earth observation, a new generation of space-based IoT is emerging, capable of connecting objects in the most remote areas: at sea, in the mountains, in agricultural areas, on critical infrastructure or across extensive energy networks. Global tracking of logistics assets, precision farming, monitoring of energy networks, natural resource management, detection of anomalies or environmental events: use cases are multiplying. But this promise also raises questions: costs, latency, data volume, integration with existing systems, cybersecurity, and dependence on space operators. Is space-based IoT set to complement – or even compete with – traditional terrestrial networks? In which scenarios is it truly relevant? And how can it be integrated into a global IoT architecture combining terrestrial and space-based systems?

© BLACKNBLUE MARKETS 2026

Industrial simulation: powered by AI, digital twins are scaling up

Fabrice Deblock,
Christophe Eschenbrenner, Dassault Systèmes
Anuchika Stanislaus, Secrétariat Général pour l'Investissement / France 2030
Pascale Vicat-Blanc, INRIA

Simulation and digital twins are no longer merely engineering tools used during the design phase. They are gradually establishing themselves as operational tools for managing production, optimising performance, anticipating breakdowns, testing industrial scenarios and training operators. But their large-scale deployment remains a challenge: model complexity, data quality and availability, implementation costs, and integration with existing systems. Artificial intelligence could be the game-changer. By making it easier to create models, utilising industrial data more effectively, automating certain simulations and enabling simpler interactions with users, AI paves the way for digital twins that are more accessible and more widely deployed across the organisation. But are we really at a tipping point? Can digital twins evolve from expert tools into industrial tools deployed at scale? Which use cases are actually working today? What are the technical, economic and organisational barriers? And what skills will be needed to make the most of these new tools?

Plenary Session, Wednesday Afternoon
Are humanoid robots ready to make their debut in factories?

Julien Bergounhoux, L'Usine Digitale
Camille Croze, Wandercraft
Laurent Duthoit, Renault
Emanuela Girardi, AI, Data & Robotics Association
Abderrahmane Kheddar, CNRS
Philippe Souères, CNRS
Pierre-Brice Wieber, INRIA

Humanoid robots, capable of moving around, handling objects and interacting with their environment, have captured the imagination for decades. Today, certain innovations promise to integrate them into production lines and warehouses. Their potential is enormous: addressing labour shortages, automating complex tasks, reducing the physical strain of work and improving industrial flexibility. But the technological reality remains challenging. Reliability, safety, cost and integration into mixed environments with human operators: these are all challenges that are holding back their widespread adoption. Are humanoid robots ready to work alongside humans? Which industrial processes can truly benefit from their presence? And how can teams and organisations be prepared for this radical transformation? Capabilities and limitations, use cases: can humanoid robots find their place in factories?

BNB markets. *Humanoid robots are not ready to replace human workers, but the race is on and Europe is not behind on technology, only on money. Laurent Duthoit said everyone is at roughly the same level, and that China is mostly focused on its home market. Renault, active in industrial robotics for five years,*

© BLACKNBLUE MARKETS 2026

is both a maker and a user of robots, with manufacturing now handled by Wandercraft. The company struggles to recruit young workers, for example for the third R5 line in northern France. It works with sociologists so that people work alongside robots rather than being replaced, since there are real social fears, as shown by the strike at Hyundai. Technical limits remain: motors overheat after about two hours, and sensors that detect a heartbeat are being considered to tell humans and machines apart.

Fabien Expert and Emmanuel Girardi pointed to the funding gap: €1 billion invested in France versus €100 to 110 billion in China, and even more in the US. Rather than an all-purpose robot, the strategy with Renault is a robot that does one task very well. Robots learn by watching hundreds of people perform tasks on video, combined with AI. Europe needs its own standards for physical AI, possibly a "Robotics Act" as part of the AI Act.

The researchers added perspective. Pierre-Brice Wieber said the real challenge today is fine, complex manipulation. Abderrahmane Kheddar noted that no robot can yet do what industry needs. He added that comparing Europe with China makes little sense socially, because young Chinese people no longer want factory jobs and China does not rely on foreign labour. He also wants industrial research centers placed at the heart of universities. Philippe Souères explained that progress in electric motors, driven by drones and EVs, has fuelled humanoid robots. He warned of two hidden risks: mass-producing robots before their value-added tasks are proven, and losing human know-how that robots will not pass on. The message to all: connect startups and laboratories, and act now.

How yesterday's 'Security by Design' approach supports your compliance with the Cyber Resilience Act 2027

Tony Ducrocq, Decathlon SE
Julien Littler, Decathlon SE

In December 2027, with the Cyber Resilience Act (CRA), the rule will be clear-cut: a non-compliant connected product will simply no longer be allowed onto the European market. For manufacturers, the impact on turnover is direct. Yet cybersecurity is still too often perceived by business units as a cost centre that slows down product launches. In this case study, discover how a sports retail company anticipated this legal requirement and turned it into a competitive advantage. Through the combined perspectives of a Regulatory Affairs Manager (who breaks down the law and standards) and an Engineer (who implements solutions and supports the product teams), we'll share a pragmatic and people-centred approach. Forget the technical jargon: we'll show you how to balance security and profitability, from the initial risk analysis to managing your software supply chain. A practical guide to turning the CRA into a business accelerator.

BNB markets. *From December 2027, under the Cyber Resilience Act (CRA), a connected product that does not comply will simply be banned from the European market, which directly threatens revenue. Decathlon shared how it prepared early and turned this constraint into a competitive advantage. With more than 100,000 connected products in circulation, the brand knows its exposure. It learned from past failures such as the Quechua phone, and from the risk of seeing devices with default passwords like "admin:admin" hijacked into botnets.*

Its approach is to build security in from the start: every connected product goes through a rapid cyber risk assessment before launch. Decathlon also learned from the UK, whose PSTI law was the world's

© BLACKNBLUE MARKETS 2026

first cybersecurity law for consumer connected products, together with the Code of Practice for Consumer IoT Security.

The CRA is a paradigm shift. It sets both functional and contractual requirements and covers every component of the product, which makes managing the software supply chain essential. It also has very concrete requirements, such as information to include in the user manual and a way for users to delete their data. The key message: treat cybersecurity as a business accelerator rather than a cost center, with a pragmatic, people-centered approach that brings regulatory experts, engineers and product teams together.

AI and Cybersecurity: How far should we go with automation?

Charles d'Hondt, Lexfo
Fabrice Deblock,
Laurent Hausermann, CyGO Entrepreneurs
Ludovic Lecomte, Santevet
Alexandre Marguerite, Devensys Cybersecurity
Jean-Luc Marini, SRA

Artificial intelligence is rapidly transforming the cybersecurity sector. Anomaly detection, log analysis, incident response, alert triage, investigation, patch generation, attack simulation: more and more tasks can be automated, either partially or entirely. Faced with a shortage of cybersecurity experts and an explosion in the number of alerts, automation appears to be an essential solution. But to what extent can cybersecurity really be automated? Can we allow AI to isolate a production system, block a user, or trigger an incident response without human validation? What are the risks of errors, false positives and poor automated decisions? And how can we maintain control over increasingly autonomous security systems? Between gains in efficiency, reduced operational burden, improved detection and new risks associated with automation, organisations must strike the right balance.

Your experts' knowledge shouldn't leave with them

Gilles Faurie, Precia Molen
Lucas Nacsa, Neovision

In industry, far too much knowledge is not found in procedures or manuals, but in the minds of those who have been in the trade for years. Techniques, instincts, tips, habits, decision-making criteria… all this knowledge risks being lost when an expert leaves. Drawing on real-world experience, this workshop will demonstrate how to identify and capture the knowledge held in experts' minds, supplement it with existing company documents and discussions, and then make it easily accessible to teams using AI. The aim is to preserve the company's know-how, retrieve the right information, understand past decisions and gain greater autonomy, even when the expert is no longer there.

© BLACKNBLUE MARKETS 2026

IT reversibility: a key driver of digital and industrial resilience?

Isabelle Bouvier, Bouvier Avocats
Maxence Cossalter, Anima Conseil
Maxime Duprez, Visiativ
Hervé Groléas, Métropole de Lyon

Cloud, SaaS, IoT platforms, cybersecurity solutions, business software, outsourced infrastructure… Businesses have never been so dependent on technology providers. Against this backdrop, IT reversibility – that is, the ability to switch providers, repatriate data, migrate applications or rebuild a system elsewhere – is becoming a strategic issue for digital and industrial resilience. But is reversibility a reality or a theoretical concept? How can it be anticipated right from the solution selection phase? What are the technical, contractual and financial barriers? How should the portability of data, applications, configurations and AI models be managed? And what is the true cost of non-reversibility?

PLC virtualisation: towards a new era in industrial automation?

Marcos Didonet Del Fabro, CEA-List
Jean-Philippe Malicet, Cap'Tronic
Claude Miot, Schneider Electric
Fred Rivard, MicroEj

For a long time, industrial automation relied on physical controllers installed as close as possible to machines and production lines. But with the rise of virtualisation, edge computing and the industrial cloud, a new approach is emerging: that of virtualised controllers, capable of running on standardised IT infrastructure rather than on dedicated hardware. This development opens up new possibilities: greater flexibility, faster deployments, simplified updates, shared infrastructure, reduced dependence on hardware, and easier integration with IT systems, data and artificial intelligence. But it also raises new questions: real-time performance, cybersecurity, resilience, network dependency, required skills, and the evolving role of automation engineers. Does the virtualisation of PLCs mark a paradigm shift comparable to that of server virtualisation in IT? Are we at the beginning of a profound transformation of industrial automation? What use cases are already in production, what are the obstacles, the risks, and the real benefits for manufacturers?

Are you sure that no data breaches are exposing your business to cybercriminals?

Thierry Gourdin, Kaspersky

As your IT environments expand, your organisation exposes more digital assets: websites, applications and shared data. This growing digital footprint increases risks and presents new opportunities for cybercriminals, who are becoming ever more sophisticated. It is therefore crucial to gain an accurate picture of your online presence so that you can respond quickly to threats. Discover how Digital Footprint Intelligence helps you regain control: continuous monitoring of your external exposure, early threat detection and active protection of your brand, going far beyond traditional tools. How do cybercriminals exploit companies' digital footprints? How does DFI map your exposure and identify

© BLACKNBLUE MARKETS 2026

critical risks? How does a clear view of your external surface area become a key tool for prevention? Is your business truly protected online? Who can see your data and services on the internet? Could your brand be impersonated without you even realising it?

Adopting robotics: before the technology, consider design and usage

David Gal-Reignez, Minalogic
Arnaud Huille, Navya Mobility
Louis-Romain Joly, SNCF
Anne Pellegrin, Auvergne-Rhône-Alpes Entreprises

Many robotisation projects fail or fall short, not because of the technology, but because their intended uses were poorly defined from the outset. Attempting to integrate a robot into an existing process without rethinking the organisation, workflows, workstations or user experience often leads to complex, costly and unprofitable projects. What if the real question wasn't "which robot to choose?" but "what problem do we want to solve, and how can we rethink the process?" Workstation design, ergonomics, human-machine interaction, operator acceptance, workflow organisation, safety, training: robotics is as much about design and usage as it is about technology. Discover why robotisation projects must first be designed with usage in mind, and how to adopt a "design to automation" approach rather than a "technology first" one.

Smart sensors: how far can we go in terms of energy self-sufficiency?

Pierre Gelpí, E-Peas
Florence Lis, Orioma
Julien Musset, F2A
Emmanuelle Paquier, Cap'Tronic

Sensors are at the heart of the connected industry, smart buildings, infrastructure and connected cities. But their large-scale deployment raises a very practical question: that of power supply. Laying cables, replacing batteries and maintaining thousands of sensors in the field represents a significant cost and a major operational constraint. In response to this challenge, new approaches are emerging: low-power sensors, energy-efficient communication protocols, energy harvesting (recovery of thermal, vibrational and light energy), new generations of batteries, ultra-low-power electronics, and embedded intelligence capable of processing data locally to limit data transmission. How far can we go in terms of sensor energy autonomy? Can we envisage sensors that are fully autonomous for several years? For which use cases? What are the technological and economic limitations? And what are the implications for the architecture of IoT systems and for maintenance?

From Hardware to Intelligence: the future of ecosystem automation

Alexander Jonke, U-Experten

Discover how artificial intelligence is redefining the 'phygital' product ecosystems of the future. The automation of these ecosystems is the missing link between today's hardware and tomorrow's value creation: it drives productivity gains, paves the way for new business models and reduces waste.

© BLACKNBLUE MARKETS 2026

Drawing on the latest advances in embedded, cloud-based and hybrid AI, this workshop presents U-Experten's perspective on intelligence integrated into physical products and demonstrates how this transformation is redefining both the scope of product development and the profitability of product portfolios. Companies that understand and embrace this evolution will become the leading equipment manufacturers of tomorrow.

Can Agentic AI be used to support industrial processes?

Isabelle Bouvier, Bouvier Avocats
Fabrice Deblock
Laurent Herbillon, Fair
Paul-André Migeon, Cleverdist
Fayçal Rezgui, Araïko
Alain Vafiadès, Allioss

Following analytical AI and generative AI, a new phase appears to be emerging: Agentic AI. Capable of planning actions, interacting with multiple systems, making decisions based on objectives and performing tasks autonomously, these intelligent agents could transform the way industrial operations are managed: production planning, energy optimisation, maintenance, quality management, logistics and the supervision of complex facilities. But can we really entrust industrial processes to autonomous agents? How far can autonomy go? What are the risks in terms of safety, cybersecurity, reliability and liability? Which use cases are realistic today, and which are still in the realm of the future? And how can we integrate Agentic AI, industrial automation, existing systems and human supervision?

BNB markets. *Agentic AI can support industrial processes, but the human stays in charge: AI assists, people decide. Faycal Rezgui described an agent as three things: a goal, tools it chooses and orchestrates on its own to reach that goal, and a memory that keeps the context. In a factory, that memory often exists only in people's heads. At 3 a.m., a technician faces an error code the manual cannot solve, and the expert with 20 years' experience is not on shift. By describing the problem and sharing photos, the technician lets the agent build up and formalize this know-how. He added that people spend 30% of their time filling in data fields. The rule is to avoid gadget AI and use it only for problems you cannot solve today. Around 70% of an AI project is about people, so every level of the company must be involved, with data kept confidential, sovereign and secure.*

Paul-André Migeon recommended moving from pilot to scale step by step, building on each project, with a clear and ambitious goal, available data, change management and a fast time to value. Alain Vafiadès sees AI as a way to guide operators and make better decisions. Time saved must turn into real productivity, and the tool must be transparent so teams adopt it.

Laurent Herbillon warned that putting an LLM in a factory is not simple. The best place to start is a process with friction that spans several systems, such as stock, purchasing and reorder thresholds, because that is where the money is. He also warned about the US Cloud Act and "sovereignty washing." Isabelle Bouvier pointed out that an agent has no legal definition, only a technical one. Every case therefore needs a clear scope, full traceability, detailed specifications and clearly assigned liability across the whole value chain.

© BLACKNBLUE MARKETS 2026

Protection of industrial and operational data: simplifying storage and use

Thierry Daneau, Renault
Frédéric Grzesiak, Prosyst
Jean-Philippe Malicet, Cap'Tronic
Laurent Pipitone, Cyberium
Céline Redon, Aceso Conseil

Industrial companies today generate ever-increasing volumes of data: production data, machine data, maintenance data, quality data, traceability data, energy data, and data from sensors and the IoT. This data has become strategic for improving industrial performance, deploying artificial intelligence, optimising maintenance and managing energy consumption. But the more data there is, the more complex its storage, security and use become. Where should industrial data be stored: on-premises, in the cloud, or via Edge Computing? How can we balance data accessibility, cybersecurity, data sovereignty, costs and performance? How can we avoid creating more silos whilst retaining control over sensitive data? And how can we enable business units to use data easily without creating new security or compliance risks?

© BLACKNBLUE MARKETS 2026

CONFERENCE AND BUSINESS PRESENTATIONS THURSDAY SEPT.17

Edge AI vs Cloud AI: where should the intelligence be located?

Steven Dolbeau, Anima Conseil
Sébastien Dubois, Seven Lakes
Clément Gutierres, Hâpy Services
Charly Hamy, Rtone
Arnaud Jaoul, Alstom

Artificial intelligence is becoming central to industrial systems, but a key question remains: where should data be processed and models run? In the cloud, to benefit from computing power and scalability? Or as close to the field as possible, via edge computing, to reduce latency, limit data flows and ensure operational continuity? Between Edge AI and Cloud AI, the choice is not merely technical. It involves considerations of performance, costs, cybersecurity, sovereignty, energy consumption and integration with existing systems. Some applications require a real-time response, whilst others demand massive learning or storage capabilities. In practice, hybrid architectures are becoming increasingly common… but their implementation remains complex. What use cases truly justify Edge AI? When is the Cloud still indispensable? How should one balance centralisation and distribution of intelligence? And how can one build a coherent, scalable and secure architecture?

Industrial hyper-automation: synchronising and securing your IT and OT operations with ServiceNow

Martin Croville, Devoteam
Neil Thomas, ServiceNow

Industry 4.0 is based on a powerful promise: the complete convergence of information technology (IT) and operational technology (OT). However, digitising production lines – some of which are ageing – exposes factories to new vulnerabilities. How can you carry out this transformation without disrupting your value chains? The answer lies in hyper-automation. This workshop invites you to discover how ServiceNow is establishing itself as the true backbone of your operations. We will explore asset management and the security of industrial systems, drawing in particular on Armis's expertise to map and protect OT, in order to effectively orchestrate incident response and on-site interventions. Gone are the days of manual, disjointed processes: make way for centralised, seamless management. Illustrated with real-world use cases and feedback, this session will give you the keys to accelerating your digital transformation, securing your sites and optimising the full lifecycle of your most strategic equipment.

AI: how can we speed up the remediation of vulnerabilities whilst maintaining the stability of IT systems?

York Von Eichel-Streiber, NinjaOne

In the age of AI, vulnerabilities are being detected, prioritised and sometimes exploited at an ever-increasing pace. For IT and security teams, the challenge is no longer simply to identify vulnerabilities,

© BLACKNBLUE MARKETS 2026

but to fix them quickly, without causing instability or disrupting operations. Using a real-world use case, this workshop will demonstrate how to improve visibility across endpoints, prioritise the most critical vulnerabilities and automate remediation actions in a controlled manner. The aim is to reduce risk exposure whilst maintaining IT system stability and business continuity.

IoT, analytics, AI and digital twins: the cornerstones of a zero-defect industrial approach?

Nicole Briand, Inouid
Maxence Cossalter, Anima Conseil
Cédric Jarkovsky, Transatel
Mohamed-Lamine Messai, Université Lumière Lyon 2
Richard Salvetat, Cap'Tronic

IoT sensors, big data, advanced analytics, artificial intelligence, simulation and digital twins: digital technologies promise to transform industry towards a new model – the 'zero-defect' model. Early detection of deviations, predictive maintenance, automated quality control, process simulation and real-time optimisation: data is becoming the heart of industrial management. But is this promise of zero defects realistic? Which technologies are actually creating value today? Should we start with the IoT, with data, with AI, or with simulation? How can these technological building blocks be integrated with one another? What are the prerequisites in terms of data quality, infrastructure and skills? And what returns on investment can we expect?

BNB markets. *Zero defects is not a technology you buy, it is a target reached through structured continuous improvement, and everything rests on reliable data. Nicole Briand (INOUID), an IoT solutions integrator, explained that the job is to pick the right sensors and data for each need and make the data speak through machine learning. It is not only about new sensors: much of the value lies in existing data that can help people. Projects are built with the client around real use cases. They start with a pilot that checks the data against reality on the ground: a pilot takes about 6 months, and a full project 12 to 18 months, like an IT project. Richard Salvetat (CAP'TRONIC) added that linking people, machines, sensors and data depends above all on business expertise.*

Mohamed Lamine Messai (Université Lyon 2) focused on data accuracy and reliability along the whole chain, from collection to use. Digital twins can simulate an attack on a network, such as a home network, to find which device is the weak point. Each case must be put in context, because every client has specific needs. He warned about data poisoning, which produces biased models. Offline training is easier to control, while federated learning is riskier and needs cryptographic or similar safeguards. Quantum is also arriving, with its own protocols.

Cédric Jarkovsky (Transatel) stressed involving all stakeholders from the start, steering by data and setting up data governance, so the data can feed continuous improvement. Every infrastructure layer that carries data must be planned, with a highly resilient network aiming for 99.9% uptime. He cited Airbus and BMW as good examples, and the Cyber Resilience Act came up again. His conclusion: connectivity must be resilient at every level.

© BLACKNBLUE MARKETS 2026

Combating fraud and financial cyber risks for SMEs and mid-market companies

Jérémy Asta Vola, AVCA Legal
Denis Boyer, Cybermalveillance.gouv.fr
Laurent Camus, RECyM
Fabrice Deblock,
Alix Durand, ANSSI
Guillaume Santiago, Onlynnov

Cyberattacks targeting financial gain are skyrocketing, with SMEs and mid-market companies bearing the brunt: CEO fraud, fake bank details, email compromise, ransomware extortion, and the diversion of supplier payments… These attacks, which are often meticulously planned, rely more on social engineering and organisational weaknesses than on highly sophisticated IT techniques. And their consequences can be catastrophic for a business. Faced with these risks, many organisations still believe that the issue is solely a matter for IT or cybersecurity. In reality, financial fraud is also – and above all – a matter of internal processes, financial control, governance, staff training and risk management. How do these frauds work in practice? Why are they so effective? What are the most common mistakes? What simple and practical measures can SMEs and mid-market companies put in place to significantly reduce their exposure to risk, without implementing overly complex systems?

Regulation, funding, supply-side policy: how can Europe accelerate its transition to automation?

Cibil Alysée, CIMES
Emanuela Girardi, AI, Data & Robotics Association
Marie Leynaud, Deuxième Écoute
Philippe Mattia, Le capital risque en France
Catherine Simon, Secrétariat Général pour l'Investissement / France 2030

Whilst robotisation is emerging as a key driver of competitiveness, reindustrialisation and a response to labour shortages, Europe still lags behind other major industrial regions, particularly Asia. Yet the stakes are high: industrial sovereignty, productivity, working conditions, demographic transition and the relocation of certain production activities. The issue is no longer merely technological, but also economic and political. How can we remove the barriers to investment in robotics, particularly for SMEs and mid-market companies? Are the funding schemes appropriate? Is European regulation a hindrance, or can it become a competitive advantage? Is there a need for a genuine industrial policy on robotisation in Europe, similar to what has been done for other strategic sectors?

© BLACKNBLUE MARKETS 2026

Plenary Session, Thursday Morning Cybersecurity: Agentic AI, a friend who (doesn't) mean you (only) well?

Fabrice Deblock
David Garcia, Groupe Casino
Étienne Lacour, Microsoft Security
Pierre Parrend, EPITA
Maricela Pelegrin-Bomel, Établissement Français du Sang
Aldrick Zappellini, Crédit Agricole

Agentic AI, capable of acting autonomously, performing tasks, making decisions and interacting with information systems, opens up new possibilities for businesses: automation of security tasks, faster incident response, big data analysis, support for IT teams… But these new intelligent agents also represent an unprecedented attack surface: manipulation of agents, compromise of automated workflows, data exfiltration, decision-making errors, or even exploitation by attackers to automate cyberattacks. In this context, will Agentic AI strengthen corporate cybersecurity or create new risks that are difficult to manage? Between the promise of automation, productivity gains, technological dependency and new attack scenarios, how can these technologies be integrated whilst maintaining control?

BNB markets. *Agentic AI is both a powerful lever and a new attack surface. The key is to frame it without stifling it, keeping strict control over what agents can see and do. David Garcia (Groupe Casino) said AI projects now come from every department, and the cure must not be worse than the disease. The challenge is to move fast while legal and policy teams slow things down and requests keep changing before they are approved. Access rights are critical: an agent that reads every message can find information it should never see.*
Aldrick Zappellini (Crédit Agricole) described a nuanced level of maturity. One team's agent can be reused by sister teams, but in banking and heavy industry, robustness and precision are essential because every agent opens a door to attacks. Banking runs on trust, so progress must be careful, and the cost of an error must be weighed along the chain of responsibility. Maricela Pelegrain (Établissement français du sang) said the EFS moves step by step: no AI without prior analysis, starting with the most confidential and sensitive cases. She warned about shadow AI, which spreads anyway if no official tools are offered.

Etienne Lacour (Microsoft Security) called an agent a new employee and a powerful lever, but a stubborn one: blocked on the left, it will try the right. Because it wants to please, it needs strict rules, limited rights and identity controls, especially when it accesses a database in admin mode. Its behavior must also be monitored. Some actions, like prescribing a dosage, must stay reserved for authorized people. For vulnerabilities (CVEs), he pointed to Microsoft's Project Perception, an agentic platform where AI agents detect, analyze and fix security flaws. On open source, he said you need the skills to analyze it yourself. Pierre Parrend (EPITA) presented research on detecting and assessing AI risks and validating protocols. He cited ChatGPT's outages this summer as a reminder of how dependent we have become.

© BLACKNBLUE MARKETS 2026

Designing and deploying an AI model for detecting cardiac abnormalities (audio) and counting bicycles (vision) using ColibryNPU and the Aidge platform

Thomas Gillot, Asygn
Adrien Vialletelle, Asygn

Designing a smart patch for detecting cardiac abnormalities, a standalone sensor for counting bicycles, or smart wearables all involve overcoming the same challenge: running on-board AI on systems with extremely limited memory and power, often battery-powered. In this context, ASYGN's ColibryNPU is a neural processor designed to run neural networks with very low power consumption, below one milliwatt. However, it requires a key step: the compression and optimisation of models to make them compatible with embedded hardware constraints. The Aidge platform enables the design, optimisation and deployment of TinyML models tailored to embedded systems. The workshop programme includes: an introduction to the architecture of ColibryNPU, an ultra-low-power neural accelerator; a presentation of the Aidge platform for designing complete embedded applications incorporating AI; the design and deployment of a vision-based and then audio-based detection model; and a live benchmark: performance, inference times and energy consumption.

Cybersecurity: how to prepare your crisis communication strategy

Jonathan Belhocine, Direction Nationale de la Police Judiciaire
Laurence Lacombe, LDLC
Marie Leynaud, Deuxième Écoute
Yann Loubry, Parquet de Paris
Stéphanie Revol, Revol Avocat
Margaux Vincent, ANSSI

At a time when cyberattacks are no longer a question of "if" but of "when", organisations must be prepared to manage not only the technical incident itself, but also the media and reputational storm that accompanies it. Data breaches, ransomware, system paralysis: every digital crisis instantly becomes a crisis of confidence. In this context, what are the best practices for effective crisis communication? How can scenarios be anticipated? What messages should be prepared in advance? How can technical, legal and communications teams be coordinated? And above all, how can the trust of customers, partners and employees be maintained in a climate of uncertainty?

Integrating AI into production environments: why is it so complicated?

Christophe Brunschweiler, Smile
Vincent Carluer, Odiss.ai
Fabrice Deblock,
Guillaume Gimenez, 2Gi Technologie
Virginie Mathivet, Hemelopse

Artificial intelligence demonstrators are becoming increasingly impressive. However, the transition from a model that works in a laboratory or on a dataset to AI that is actually integrated into a

© BLACKNBLUE MARKETS 2026

production environment is often a long, complex and costly process. Issues with data quality and availability, integration with existing systems, real-time constraints, cybersecurity, model maintenance, data drift, business validation, and liability in the event of errors: the industrialisation of AI remains a major challenge for many companies. Why is this scaling-up so difficult? What are the main technical, organisational and human barriers? Should industrial processes be adapted to AI, or should AI be adapted to the constraints of the field? What role do MLOps, Edge AI, data platforms, simulation and digital twins play? And how can we prevent AI projects from getting stuck at the experimental stage? Discover how to move from experimental AI to industrial AI that is deployed, maintained and creates value over the long term.

Update your FPGA/SoC with the latest MPU+FPGA from NXP and Lattice

Franck Perronnet, Lattice Semiconductor
Christophe Rapine, NXP

FPGA/SoC are costly to develop and maintain, hence they lack scalability and new roadmaps. Now is the time to consider an Up-To-Date SoC ecosystem, with the latest security and AI capabilities, and supply chain resilience. NXP and Lattice have partnered to bring the best of MPUs (roadmap, ecosystem, firmware support) with leading low power and secure FPGAs. Both partners will bring reference designs to help customers jump start their projects, and SoM modules to enable fast Proof-of-Concepts and small volume production needs. The first reference design on PCIe is demonstrated on our common booth at the SIDO 2026 for the first time. Come and see how your next project can benefit from new standards/interfaces, with efficient, flexible I/O and targeted acceleration, while adopting hardware security and PQC.

BNB markets. *NXP and Lattice have partnered to help manufacturers replace aging all-in-one FPGA/SoC chips, such as Xilinx Zynq or Altera Cyclone families, with an up-to-date pairing: a modern NXP processor plus a low-power Lattice FPGA. Franck Peronnet (Lattice) explained that the FPGA can act as the main chip or as a companion chip. Lattice is a pure FPGA player focused on the lowest possible power, and the world's number one in FPGA volume. With NXP as the processor leader, customers get the latest ecosystem, roadmap and firmware support, and the interface and latency between the two chips are the key. The first joint reference design pairs an NXP i.MX 95 processor with a Lattice Nexus FPGA over PCIe, offloading real-time processing, sensor aggregation and protocol bridging from the main CPU.*

The major announcement is Lattice Prompt, an AI design assistant launched in September 2026. FPGA engineers describe their design in natural language and the tool runs the full Lattice Radiant flow: simulation, synthesis, place and route, timing analysis and bitstream generation. It works with the developer's choice of AI model and coding tool, including Claude Code, Cursor and Visual Studio Code, claims productivity gains of 10x or more on common tasks, and is a free download.

Christophe Rapine (NXP) focused on competitiveness, productivity and security. The buzzword used to be 5G; today it is AI. He traced how computing moved between data centers and the edge from 2000 to 2025 and concluded that the right system architecture is the one tuned to the actual need.

© BLACKNBLUE MARKETS 2026

BNB markets. FPGA/SoC Market: Towards More Flexible and Modular Architectures

The NXP/Lattice partnership illustrates a broader transformation of the FPGA market, expected to grow from approximately $11.7 billion in 2025 to $19.3 billion by 2030. Traditionally dominated by integrated FPGA/SoC architectures from AMD/Xilinx and Altera, the market is increasingly driven by the need for flexibility, lower power consumption, cybersecurity and faster development cycles.

By combining an NXP application processor with a low-power Lattice FPGA, the two companies propose an alternative to traditional all-in-one solutions. This modular architecture could facilitate product upgrades, extend equipment lifetimes and reduce dependence on a single semiconductor roadmap. However, its competitiveness will depend on total system costs, integration complexity and communication performance between the two chips.

Competition remains intense. AMD continues expanding its Zynq and Versal portfolios, Altera is developing its Agilex families, while Microchip targets low-power and security-sensitive applications with PolarFire SoC. Meanwhile, AI-assisted FPGA development tools, such as Lattice Prompt, are emerging as a new competitive differentiator.

The key takeaway is that FPGA competition is shifting from individual chip performance towards complete system architectures, software ecosystems and long-term industrial flexibility.

For a more detailed analysis of the FPGA market, the NXP/Lattice strategy and its competitive positioning against AMD, Altera and Microchip, see the dedicated article **“FPGA and SoC Market: The Battle Between Integrated and Modular Architectures”** at the end of this report.

Robot as a Service (RaaS): towards on-demand robotics?

Steven Dolbeau, Anima Conseil
Thierry Giraudet, Sphynx Industrie
Charles Justal, Robloc
Antoine Rennuit, Les Companions

The Robot as a Service (RaaS) model promises to transform access to robotics, particularly for SMEs and organisations that do not wish to invest heavily in expensive equipment. Based on the SaaS model used in software, RaaS would allow users to pay for a robot on a pay-as-you-go basis, via a subscription or service, sometimes including maintenance, updates and even operation. But does this model deliver on its promises? Is it truly more flexible and accessible, or simply more expensive in the long run? Which types of robots and applications are best suited to the RaaS model: logistics, cleaning, inspection, collaborative robotics, mobile robotics? How should the overall cost be assessed? Who bears the risks? And what are the implications in terms of integration, maintenance, cybersecurity and data management?

© BLACKNBLUE MARKETS 2026

Securing your industry: the Cyber Auvergne-Rhône-Alpes initiative

Carine Duwat, Auvergne-Rhône-Alpes Entreprises
Guilhem Giraud, CSIRT Cyber Assistance Auvergne-Rhône-Alpes
Margaux Mérieux, Campus Région du Numérique
Lionel Poinsot, Experts du Numérique en Entreprises (ENE)
Mickaël Villain, Région Auvergne-Rhône-Alpes

Auvergne-Rhône-Alpes has set itself an ambitious goal: to become a European leader in industrial cybersecurity. The first step in its roadmap is the creation of a regional Cyber Campus, designed as an operational base for manufacturers seeking to secure their production lines, data and workforce. In 45 minutes, discover how the regional ecosystem is mobilising its resources – assessments, funding, technology platforms, training and networks – to enable SMEs and mid-market companies to take action to improve compliance and cybersecurity.

Chatbots, co-pilots, AI agents: what two years of real-world experience have really taught us

Virginie Dotta, Sopra Steria
Floriane Samson, Sopra Steria

After two years of rolling out Microsoft tools (chatbots embedded in M365, Copilot Studio, GitHub Copilot, Azure AI Foundry), one thing is clear: the real challenge is no longer to experiment with AI, but to successfully scale it up and integrate it into our IT systems. This conference offers practical insights into how usage has evolved, from the first AI assistants to agents capable of interacting with the processes, data and applications of information systems. We will share key lessons learnt: observed benefits, limitations encountered, conditions for success, new cyber risks, governance challenges and best practices for scaling up AI without compromising security.

Edge AI and Agentic AI: is embedded AI more energy-efficient?

Laure Alfonsi, Green IT
Benjamin Cabé, Linux Foundation
Philippe Lanney, Quectel
Gillo Malpart, Mavana.earth
Pietro Maris Ferreira, Université Savoie-Mont-Blanc

As artificial intelligence becomes increasingly widespread across all systems, one question arises: where and how should these models be run in a sustainable manner? Between resource-hungry AI deployed in the cloud and edge AI deployed as close as possible to the field, a new path is emerging. Combined with Agentic AI approaches capable of making decisions and taking action locally, edge AI promises to reduce data flows, optimise processing and improve responsiveness. But is this promise of efficiency a reality? Does Edge AI genuinely reduce the overall energy footprint, or does it simply shift consumption to thousands of distributed devices? What are the trade-offs between performance, power consumption, latency, maintenance and complexity? And in which scenarios does embedded Agentic AI deliver real value compared to centralised architectures?

© BLACKNBLUE MARKETS 2026

AI: Build your own system or buy an off-the-shelf solution?

Thierry Alvergnat, Acuytiv
Yohann Burgan, Alixio Group
Laura Cozzolino, Neoresilia
Gaëtan de Sainte-Marie, Qantis
Quentin Giraud, Racoon.ai
Guilhem Lefranc-Morin, IT Novem (Groupe SNCF)

With the rapid rise of artificial intelligence, businesses face a pivotal decision: should they develop their own models and tools in-house, or rely on existing solutions offered by software vendors, system integrators or cloud platforms? Behind this question lie major strategic issues: data control, model customisation, costs, deployment times, in-house expertise, technological dependency, cybersecurity and reversibility. Does in-house development really enable a company to stand out? Are 'off-the-shelf' solutions sufficient for most use cases? How should one choose between open source, proprietary solutions and cloud services? And how can one avoid launching complex and costly projects with no guarantee of a return on investment? The aim of the round table: to help decision-makers make informed choices between build, buy or hybrid, depending on their strategy, their resources and the actual value expected from AI.

Industry 4.0: turning advanced technologies into a real driver of productivity for small and medium-sized enterprises (SMEs) and mid-market companies

Vincent Charlet, La Fabrique de l'Industrie

Robotics, AI, digital twins, 3D printing, connected devices… for over a decade, advanced technologies have been promising to boost industrial productivity. But what is really happening in European SMEs and mid-market companies? Drawing on an original survey of 1,200 SMEs and mid-cap companies in France, Germany and Italy, Vincent Charlet will share his key findings on the uptake of advanced technologies in industry. French companies are not currently lagging behind their neighbours in terms of technology adoption, but they could fall behind as their investment plans remain less ambitious in the run-up to 2030. Furthermore, technology does not automatically lead to productivity gains: it boosts performance only when accompanied by skills development and organisational improvements. A keynote speech to understand how to turn Industry 4.0 into a real competitive advantage for industrial SMEs and mid-cap companies.

Can we measure the return on investment from cybersecurity measures?

Denis Boyer, Cybermalveillance.gouv.fr
Laini Cultier, CEFCYS
Fabrice Deblock
Corentin Paimparé, Howden Group
Thierry Rouquet, Digital League

Cybersecurity is often seen as a cost centre, insurance against an uncertain risk, or a regulatory requirement. Yet companies are allocating ever-increasing budgets to it: security tools, audits, training,

© BLACKNBLUE MARKETS 2026

monitoring, vulnerability management, regulatory compliance, cyber insurance… One question regularly arises in senior management and finance departments: what is the return on investment for cybersecurity? But can we really measure the ROI of an incident that never happened? How can we assess avoided losses, gains in resilience, risk reduction, improved customer confidence, or even the impact on the company's reputation? Are there relevant indicators for steering cyber investments? How should one prioritise between multiple security investments? And how can a cyber risk be translated into financial indicators that are understandable to senior management or the finance department?

Extended realities: a new step towards the immersive factory?

Frédéric Borrel, Volvo
Maxime Dumas, Persitant Studios
David Gal-Reignez, Minalogic
Romain Pinquié, Université Grenoble Alpes - Grenoble INP

Virtual reality, augmented reality, mixed reality: extended reality (XR) technologies promise to transform a wide range of industrial applications — operator training, assisted maintenance, collaborative design, simulation, remote support, data visualisation, digital twins… For several years now, the number of proof-of-concept demonstrations has been growing, but large-scale deployments remain limited. Is extended reality reaching a turning point thanks to improved equipment, falling costs and integration with digital twins and industrial data platforms? Which use cases are actually working today? What are the obstacles: ergonomics, user acceptance, cybersecurity, integration with existing systems, return on investment?

BNB markets. *Extended reality (XR) has been promising to change industry for years, but most projects still stop at the pilot stage. A recent review of 80 studies found that large-scale use in maintenance is held back as much by organization and human factors as by technology. Things are moving, though: hardware is getting cheaper and easier to use, and no-code tools now let engineers build XR content themselves. Regulation is helping too: from January 20, 2027, the EU Machinery Regulation allows machine instructions to be supplied in digital form.*

Frédéric Borrel (Volvo Group) works on scaling up AR, VR and mixed reality across the group, with CAD/PLM data continuity and digital twins as the foundation. He also co-organizes the XR Days at La Ruche Industrielle in Lyon. He has warned that the ideal headset for industrial AR still does not exist.

Maxime Dumas (Persistant Studios) co-founded the studio behind PopcornFX, a real-time visual effects engine used in big video games and in XR projects, for example with Magic Leap. He argues for open standards such as USD. David Gal-Régniez (Minalogic) leads the cluster's creative industries, NewSpace and robotics communities, and helps members find funding for their innovation projects and Romain Pinquié (Grenoble INP UGA, G-SCOP lab) co-leads GAIA XR, a France 2030 project with Skyreal and CEA-List. It aims to build Europe's first unified collaborative platform for working on product data throughout a product's life cycle.

© BLACKNBLUE MARKETS 2026

Water, lighting, buildings: how can we measure the indirect environmental benefits of IoT technologies?

Benjamin Bailly, Voltalis
Fabrice Deblock,
Gillo Malpart, Mavana.earth
Cyril Masson, KPN IoT
Richard Salvetat, Cap'Tronic

IoT projects in buildings, street lighting and water management are often presented as drivers of the green transition: reducing energy consumption, optimising resources, improving maintenance and extending the lifespan of equipment. But beyond direct savings, these technologies also generate indirect environmental benefits that are harder to measure: fewer maintenance trips, better infrastructure management, reduced water wastage, more precise adaptation to actual usage, and more accurate consumption control. How can these indirect environmental gains be measured? What indicators should be put in place? Should we consider life-cycle analysis, carbon footprints, resource savings, or the impact on the lifespan of equipment? How can we ensure that digital technology deployed for optimisation does not itself become a source of additional environmental impact?

Dealing with agentic AI threats: understanding and anticipating new risks

Étienne Lacour, Microsoft Security

The emergence of agent-based AI systems is profoundly transforming digital environments… but also the threat landscape. These new capabilities – which are autonomous and interconnected – pave the way for unprecedented attack scenarios, exploiting expanded and often still poorly managed attack surfaces. During this session, we will analyse the main risks associated with these agent-based models, using real-world examples and trends observed in the field. We will also discuss the defensive strategies to adopt in order to anticipate these threats and sustainably strengthen organisations' resilience. Finally, we will outline how Microsoft is addressing these challenges through an integrated, end-to-end security platform, designed to protect hybrid environments, identities, data and AI applications in a consistent and proactive manner.

Is AI moving fast? All the better. Take back control: let's build your agent together

Rali El Kohen, Moon by DFM

AI is advancing fast – very fast – and it's normal to feel overwhelmed. But the real question is no longer whether you're going to get started. Your competitors have already done so. The only question that matters today is: how quickly are you going to get started? The good news is that you don't need to be an expert. The real key – accessible to everyone – is knowing how to use the tool effectively. And it all comes down to the prompt. In this workshop, Moon by DFM will demonstrate this to you live. We'll show you the dramatic difference between a slapdash prompt and a well-crafted one. Then, right in front of you, we'll build an agent that reads your emails, flags the urgent ones, summarises them and sends the key points to Teams. A fully functional workflow, up and running the very next day. You

© BLACKNBLUE MARKETS 2026

won't leave with empty promises, but with a method, prompts, and the desire to take back control. Do you have a specific scenario in mind? Come and talk to us about it after the session.

BNB markets. *The message was simple: you don't need to be an expert to get started with AI, but you do need to learn to use the tool well, and that comes down to the prompt. Rali El Kohen (Moon by DFM) showed live how much better a well-built prompt is than a careless one. A key tip: ask the AI to question you first, so it can frame your need before it starts working.*

He then built an "urgent email" agent with Claude, which works in the browser, on desktop, inside Office and with connectors to other apps. The prompt follows four steps: read my emails, spot the urgent ones, summarize them, and post the key points to Teams. The result is a working workflow that can be used the very next day.

Moon is the AI arm of DFM, an independent French group founded in 2002. DFM serves more than 10,000 clients across IT, telephony, printing and document management, security and AI. DFM also sells its DFM 360 offer of turnkey technology solutions. Moon helps SMEs and mid-sized companies with AI audits, Qualiopi-certified training and custom agents. Its training catalogue includes upcoming remote sessions such as "Claude x Excel" and "Claude Cowork". Overall, a very hands-on workshop for learning how to build an agent with Claude.

Maintenance of safety conditions (MCS): a key driver of resilience

Franck Bonnard, NXO
Maxence Magnien, I-Tracing
Jean-Christophe Marpeau, Cap'tronic
Yann Mathon, MGM Solutions
Hervé Thibault, Metsys

Cybersecurity is not just about the moment a system or piece of equipment is deployed, but throughout its entire lifecycle. Security patches, software updates, vulnerability management, monitoring, end-of-life management, and access control: all these activities fall under the umbrella of Security Maintenance (MCS). Yet, in many organisations, MCS remains poorly defined, poorly managed and is sometimes confused with traditional IT maintenance. Against a backdrop of constantly evolving cyber threats, MCS is nevertheless becoming a central element of business resilience, particularly in industrial environments where systems have long lifespans and where updates are complex to deploy. Who is responsible for MCS? How should it be organised between IT, OT, production and service providers? What processes should be put in place to manage vulnerabilities and updates without disrupting production? How should actions be prioritised? What tools should be used? And how can MCS be integrated into an overall cyber risk management strategy?

Securing embedded AI: the major challenge facing connected devices

Victor Guyomard, Skyld
Vincent Richard, STMicroelectronics

Embedded (or edge) artificial intelligence is now becoming established in critical sectors such as industry, healthcare, transport and defence. By integrating AI models directly into connected devices,

© BLACKNBLUE MARKETS 2026

as close as possible to the data, businesses gain in speed and data privacy. However, whilst the security of infrastructure and data is widely taken into account, the security of the AI models themselves is still too often neglected. Yet a model deployed on a device can be extracted through reverse engineering, leading to a loss of intellectual property, risks of counterfeiting, a loss of licensing revenue, or even exposure to adversarial attacks capable of compromising its operation. Why are current software security techniques not suited to AI? What are the real risks of model theft and replication? Faced with these threats, how can an AI model embedded on a microcontroller, such as the STM32 product family, be effectively protected?

Plenary Session, Thursday Afternoon
Artificial Intelligence: are we on the brink of a job apocalypse?

Anne-Sophie Bellaiche, L'Usine Nouvelle
Amèle Douchy, Radiall
Laurence Mari, INRIA
Jean Pouly, FlexJob
Frédéric Robichon, Manpower

Artificial intelligence is advancing at an unprecedented pace. The automation of administrative tasks, content generation, IT development support, data analysis, predictive maintenance, automated customer service… No sector seems to be spared. In the face of these rapid changes, one question springs to mind: will AI destroy more jobs than it creates? Straddling the gap between the fear of a mass disappearance of jobs and the reality of a profound transformation of work, this round table aims to move beyond both alarmist and overly optimistic narratives. Which jobs are genuinely under threat in the short term? What new roles are emerging? How should businesses prepare for these changes? And above all, are we collectively ready to adapt skills, organisations and training models?

BNB markets. *The panel rejected both doom and hype: AI is not wiping out jobs overnight, but it is deeply changing work, and the first to feel it are juniors. Anne-Sophie Bellaïche reported that 10% of HR departments have already cut hiring of work-study students and junior staff because of AI.*

Laurence Mari (Inria, LaborIA) criticized studies that analyze 900 jobs and count a job as lost once 30% of its tasks can be automated. Those studies look at tasks, not at real work, which is about coordination and human interaction. Employees are positive about AI, but much of their use is hidden: 55% use it without telling their managers, and 89% of civil servants use it while hesitating to share how. She warned about hidden costs and data sovereignty. She also pointed to a weaker sense of team, as people ask AI instead of colleagues, and to AI acting as a "mirror" that confirms our ideas instead of challenging them. LaborIA, the research lab set up by Inria and the French Ministry of Labour, will publish a tool on these hidden costs in December, along with more studies on its website. Its scientific director makes the same point about colleagues interacting less.

Frédéric Robichon (Manpower) described AI agents that search candidate databases and pre-select profiles for recruiters. The real questions are whether skills evolve as fast as jobs, and what we do with the time we save: the same work with AI, or new work. Amele Douchy (Radiall) shared current uses:

© BLACKNBLUE MARKETS 2026

rewording and summarizing documents, shared assistants, non-conformity analysis and qualification reports, with competitive monitoring in development. The transition is fast but a real boost.

Jean Pouly (Flexjob) warned of the "proletarianization of white-collar workers." Like a calculator, AI augments an advanced student but replaces a beginner's thinking. Effort helps us remember and gives a sense of reward, so we need metrics that show what is really gained and what is hidden. The shared conclusion: aim for augmented, not diminished, humans, and move from a sum of individual uses to collective intelligence, where disagreement stays productive.

NIS2 for industry: take action in a methodical and confident manner

Robin Blanc, CS Group (Sopra Steria)
Nicolas Vergnes, CS Group (Sopra Steria)

The NIS2 Directive will mark a significant change for many industrial companies that have so far fallen outside the regulatory scope. This workshop presents a practical approach to preparing for the upcoming requirements: identifying the systems concerned, estimating compliance costs, prioritising actions and understanding the applicable standards. Using a methodology tailored to the resources, maturity and challenges of SMEs, mid-market companies and large enterprises, we will address the key questions: Where do I start? How should I structure my approach to prioritise human and financial resources where they will have the greatest impact? CS GROUP is organising this event, aimed in particular at industrial entities newly affected by these regulations, to transform regulatory constraints into a driver of resilience, strengthen the trust of your customers and partners, and address the challenges of digital and industrial sovereignty in a context of constantly evolving cyber threats.

European Machinery Directive: from cyber compliance to competitive advantage

Gaël Belverge, REP International
Franck Bonnard, NXO
Bruno GAIGE, SOCOTEC EQUIPEMENTS
Delphine Ghighi, Tal & Co Avocats
Charles Indriamihaja, Decathlon
Jean-Christophe Marpeau, Cap'tronic

With the new European Machinery Regulation, cybersecurity has officially become a compliance requirement for many industrial machines and systems. Access management, software updates, protection against intrusions, traceability, technical documentation and vulnerability management: manufacturers and system integrators will need to incorporate cybersecurity right from the design stage of their machines. For many companies, the issue is still perceived as a complex, technical and costly regulatory constraint. However, requirements relating to cybersecurity, software updates and machine lifecycle management can also become differentiating factors in the market: machines that are more secure, easier to maintain, more durable and better aligned with the requirements of major clients. How can these new requirements be practically anticipated? What does this mean for machine manufacturers, system integrators and industrial operators? What are the implications for machine

© BLACKNBLUE MARKETS 2026

design, architectures, maintenance, updates and documentation? And how can a regulatory constraint be turned into a competitive advantage and a selling point?

Overcoming cyber dependency: start-ups as a strategic lever for CIOs and CISO

Mathieu Berthe, Absoloote
Florian Ecard, Hackmosphere
Hervé Le Jouan, Filtar.ai
David Pekmez, SecOps Forces
Candice Petizon, Digitalberry
Sébastien Telouk, Ignitera

Faced with rising cyber risks, regulatory requirements and digital sovereignty challenges, CIOs and CISO's must rethink their technology choices. This round-table discussion will bring together innovative French start-ups to debate a strategic question: how can organisations reduce their dependence on dominant foreign solutions whilst effectively strengthening their security? Drawing on real-world experience, the speakers will share their vision of sovereignty, innovation and agility as new drivers of performance. From operational cybersecurity and digital trust to open source, AI security and even offensive security: discover how start-ups can complement, challenge and sometimes even surpass traditional approaches.

© BLACKNBLUE MARKETS 2026

FPGA and SoC Market : The Battle Between Integrated and Modular Architectures

Technology & Competitive Analysis | BNB markets | October 2026

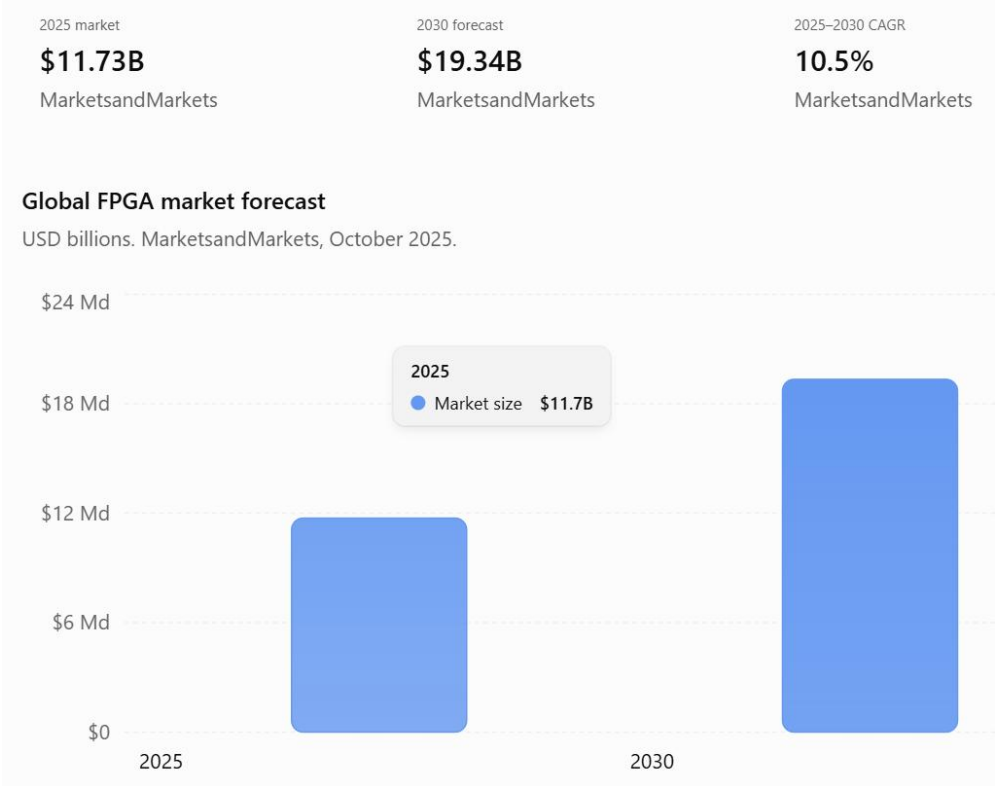
Following the NXP & Lattice presentation at SIDO Lyon 2026.

FPGA market: a growing industry facing new technological challenges

Field-Programmable Gate Arrays (FPGAs) have become essential components of many embedded electronic systems. Their main advantage is their ability to implement reconfigurable hardware functions, allowing manufacturers to adapt their products to changing requirements without designing a new ASIC.

Traditionally associated with telecommunications, aerospace, defense and industrial equipment, FPGAs are increasingly used in machine vision, robotics, medical imaging and Edge AI. These applications require a combination of parallel processing, deterministic latency, flexible connectivity and energy efficiency.

The FPGA market is expected to continue growing, although published estimates vary significantly depending on market definitions and the inclusion of FPGA-based SoCs and related devices.



Another research firm, Global Market Insights, estimates the market at $13.8 billion in 2025 and forecasts $25.7 billion in 2031, reflecting a more expansive market outlook. Meanwhile, Gartner's April 2026 analysis identifies industrial, aerospace and edge computing applications as important growth

© BLACKNBLUE MARKETS 2026

opportunities, while anticipating more limited FPGA expansion in hyperscale data centers as customers increasingly adopt dedicated ASICs.

This distinction is strategically important. The FPGA industry's growth is no longer driven solely by the pursuit of maximum computing performance. Customers increasingly prioritize power consumption, system cost, development time, cybersecurity and long-term component availability. For industrial equipment manufacturers, FPGA technology must demonstrate its economic value against increasingly powerful microprocessors, microcontrollers, GPUs and dedicated AI accelerators.

The competitive landscape is consequently evolving from a comparison of individual semiconductor components toward a broader competition between complete embedded computing architectures.

NXP and Lattice: challenging the traditional FPGA/SoC model

At SIDO Lyon 2026, NXP and Lattice Semiconductor presented a modular approach combining an NXP application processor with a companion Lattice FPGA.

The reference architecture associates the NXP i.MX 95 processor with a Lattice Nexus FPGA through a PCI Express connection. This enables the two devices to exchange data while allocating different processing tasks to the most appropriate hardware resources.

The i.MX 95 provides Arm-based application processing, real-time cores, multimedia interfaces, advanced connectivity, security functions and an integrated neural processing unit. The Lattice FPGA supplies programmable logic for deterministic operations, protocol adaptation, sensor aggregation and specialized hardware acceleration.

The partnership does not introduce an entirely new concept: discrete processors have long been combined with FPGAs in embedded systems. Its significance lies in the availability of a coordinated reference design, software resources and a development path intended to reduce the engineering effort required to integrate the two components. From a commercial perspective, the companies are addressing manufacturers that need FPGA capabilities but do not necessarily require a large, highly integrated adaptive SoC.

For NXP, the partnership broadens the range of applications addressable by its i.MX processor family. For Lattice, it creates opportunities to attach low-power programmable logic to a well-established embedded processor ecosystem. The value proposition is especially relevant to industrial systems requiring product differentiation, hardware adaptability and long operating lifetimes.

However, the modular approach introduces its own technical constraints. A two-chip design requires additional PCB space, interconnection resources, power management and system-level validation. It may also increase component procurement complexity. The central question is therefore whether the flexibility and reuse offered by the architecture compensate for its additional integration costs.

Integrated versus modular architectures: where is the economic advantage?

The competition between NXP/Lattice and established FPGA/SoC manufacturers cannot be reduced to a comparison of semiconductor performance. AMD, Altera and Microchip have developed integrated solutions combining programmable logic and processing resources within a single device. This

© BLACKNBLUE MARKETS 2026

approach offers advantages in terms of communication latency, compactness, power management and system integration. By contrast, the NXP/Lattice architecture separates the processing and programmable logic functions. Its main potential advantage is the ability to select and upgrade these resources independently. The distinction is particularly relevant when an equipment manufacturer wants to modernize an existing product while retaining specialized hardware functions developed over several years.

Comparison of the two approaches

Selection criterion	*Integrated FPGA/SoC*	*NXP MPU + Lattice FPGA*
Processing and logic integration	Single chip	Two separate chips
Interconnection latency	**Typically lower for on-chip communication**	**Depends on PCIe and software overhead**
PCB complexity	Generally simpler	Additional routing and power requirements
Hardware flexibility	**Limited to available SoC configurations**	**Processor and FPGA can be selected separately**
Upgrade possibilities	Dependent on SoC product roadmap	Potentially independent component upgrades
Software ecosystem	**Strong but vendor-specific**	**NXP software &s Lattice tools**
Component cost	One major integrated component	Two devices and supporting circuitry
Migration effort	**Potentially substantial**	**Potential reuse of processor software but FPGA logic may need porting**
Best suited for	Tightly coupled high-performance applications	Modular industrial platforms and flexible I/O

The cost advantage of either architecture depends heavily on production volumes and engineering requirements. A monolithic FPGA/SoC can reduce PCB complexity and component count. However, an equipment manufacturer may pay for processing or programmable logic resources that are not fully utilized. Conversely, a modular architecture allows more precise selection of hardware resources, but introduces additional integration costs and potentially higher board-level power consumption.

For a low-volume industrial product, development effort and long-term maintenance may be more important than the individual component price. For a high-volume application, even a small difference in the bill of materials can become decisive. The relevant comparison is therefore total cost of ownership, including component costs, engineering resources, certification, software maintenance, product upgrades and supply-chain risks.

© BLACKNBLUE MARKETS 2026

AMD/Xilinx: the strongest challenge for NXP and Lattice

AMD represents a particularly important competitor because its Zynq and Versal families have established a strong position in embedded FPGA/SoC applications. The acquisition of Xilinx in 2022 gave AMD access to a broad portfolio of programmable logic, adaptive computing platforms and development tools.

The Zynq family combines Arm processors with FPGA logic, while the more advanced Versal architecture integrates heterogeneous processing resources and specialized acceleration capabilities.

In May 2026, AMD expanded its Versal Prime Series Gen 2 portfolio with devices offering up to 100,000 DMIPS of scalar computing performance in packages as small as 23 × 23 mm. The company is emphasizing a combination of processing performance, programmable logic, multimedia acceleration and scalability across device families. This strategy directly addresses some of the arguments advanced by NXP and Lattice.

For example, AMD offers package-compatible options within parts of its Versal Prime Gen 2 portfolio, enabling manufacturers to scale processing and programmable logic resources without necessarily redesigning their printed circuit boards. AMD's principal strengths remain its established development ecosystem, high levels of integration and broad portfolio.

However, migrating from older Zynq generations to newer adaptive SoCs can still require significant software and hardware redesign. This creates an opportunity for competing architectures, particularly when customers are already considering a major product modernization.

The NXP/Lattice partnership is therefore not necessarily attempting to replace AMD in its highest-performance applications. It is more plausibly targeting selected industrial and embedded applications where modularity, low-power operation and ecosystem flexibility outweigh the benefits of tight integration.

Altera and Microchip: two different competitive responses

Altera is pursuing a broad portfolio strategy. Its October 28, 2026 announcement of Agilex 2X illustrates the company's ambition to address multiple market segments, from high-performance AI infrastructure to low-power industrial and embedded applications. The announced portfolio includes Agilex 27, 25, 23 and 22 families, targeting different combinations of computing performance, connectivity, power efficiency and I/O requirements.

Altera is also introducing QuartusIQ, an AI-assisted design environment intended to improve FPGA development productivity. Agilex 27 engineering samples are expected in the second half of 2027, making the distinction between announced products and available silicon important.

Microchip, meanwhile, follows a more specialized strategy through its PolarFire and PolarFire SoC families. Its positioning emphasizes low power consumption, reliability, security and embedded computing. PolarFire SoC combines programmable logic with a RISC-V processor subsystem, providing an alternative to Arm-based FPGA/SoC architectures.

This is particularly relevant in industrial, aerospace and defense markets, where long product lifecycles, predictable operation and security can matter more than maximum processing performance.

© BLACKNBLUE MARKETS 2026

The next competitive battlefield: software, AI and development productivity

Historically, FPGA manufacturers competed primarily on programmable logic density, operating frequency, power consumption and high-speed interfaces. These criteria remain essential, but development software is becoming an increasingly important differentiator.

At SIDO 2026, Lattice highlighted its new Prompt solution, which uses generative AI to assist FPGA development through natural-language interaction. This announcement is strategically important because the shortage of FPGA engineering expertise remains a major obstacle to wider market adoption.

AI-assisted development could reduce repetitive engineering work, accelerate design iterations and make programmable logic more accessible to software-oriented development teams. Altera's QuartusIQ announcement demonstrates that this trend is not limited to Lattice. Competition is extending toward the productivity of the entire development environment. However, AI-generated hardware designs still require rigorous verification. Functional correctness, timing closure, power optimization and safety certification cannot be delegated entirely to automated tools. For FPGA suppliers, the challenge will be to combine increasingly sophisticated silicon with development environments that reduce time-to-market without compromising reliability.

BNB markets analysis: NXP and Lattice are targeting an architectural opportunity

The presentation by NXP and Lattice at SIDO Lyon 2026 illustrates an interesting strategic development in the embedded semiconductor market. Rather than attempting to challenge AMD and Altera across the entire FPGA performance spectrum, the two companies are promoting a complementary architecture that combines a modern application processor with dedicated low-power programmable logic. The strategy appears particularly relevant to manufacturers facing the modernization of older FPGA/SoC platforms.

For these customers, the question is not simply whether a new FPGA offers higher performance. It is whether the next product generation can deliver improved processing capability, cybersecurity, AI functionality and long-term maintainability without excessive redesign costs. NXP brings an established processor roadmap, software ecosystem and embedded computing expertise. Lattice contributes programmable logic, flexible interfaces and a focus on power-efficient devices.

The partnership could also benefit from the increasing adoption of Edge AI. As intelligence moves closer to sensors and industrial equipment, heterogeneous architectures combining processors, neural accelerators and programmable logic become increasingly relevant.

Nevertheless, the commercial opportunity should not be overstated.

A discrete MPU–FPGA architecture is not inherently cheaper, faster or more energy-efficient than an integrated SoC. Its benefits depend on the application, the allocation of processing tasks, communication requirements and the ability to reuse existing software and hardware designs. Moreover, AMD and Altera continue investing in more scalable product families, advanced heterogeneous computing and improved development environments. The decisive factor for NXP and Lattice will therefore be their ability to demonstrate measurable advantages in real industrial applications, supported by reference designs, system-on-module solutions, development tools and long-term product support.

© BLACKNBLUE MARKETS 2026

The broader market trend is clear: FPGA competition is shifting from individual semiconductor performance toward complete system architectures and development ecosystems.

In this environment, the winning solution will not necessarily be the most powerful FPGA, but the architecture offering the best compromise between performance, flexibility, power consumption, engineering costs and long-term industrial sustainability.

© BLACKNBLUE MARKETS 2026

Thank you for reading and see you soon!

Lionel Touchart

SOURCES

SIDO Lyon – About the exhibition: https://www.sido-lyon.com/fr/le-salon/a-propos-du-salon
SIDO Lyon – Homepage and 2027 dates: https://www.sido-lyon.com/
SIDO Lyon – Exhibitor news (blog): https://www.sido-lyon.com/fr/actus/blog
Focus Swiss – SIDO 2026 press release (May 2026): https://focus.swiss/business/innovation/sido-2026-les-reponses-a-vos-enjeux-de-production-transformation-numerique-et-amelioration-de-process-revient-a-lyon-les-16-et-17-septembre-2026/
Lyon Entreprises – SIDO et Lyon Cyber Expo (Sept. 2026): https://www.lyon-entreprises.com/actualites/article/sido-et-lyon-cyber-expo-reuniront-8-000-professionnels-a-lyon
Mesinfos – L'industrie passe à l'échelle de l'IA (Sept. 2026): https://mesinfos.fr/69000-lyon/a-lyon-l-industrie-passe-a-l-echelle-de-l-ia-a-l-occasion-du-sido-2026-338832.html
GL events – Lyon, au rendez-vous de l'IT (Sept. 2026): https://www.gl-lyonevents.com/fr/liste-des-actualites/lyon-au-rendez-vous-de-lit
Lyon Cyber Expo: https://www.lyoncyberexpo.com/
STMicroelectronics – SIDO 2026: https://www.st.com/content/st_com/en/events/sido.html
Check Point – Cyber Security Report 2026 (Jan. 2026): https://www.checkpoint.com/press-releases/check-point-softwares-2026-cyber-security-report-shows-global-attacks-reach-record-levels-as-ai-accelerates-the-threat-landscape/
IoT Analytics – State of IoT (Oct. 2025): https://iot-analytics.com/number-connected-iot-devices/
Grand View Research – AI market report: https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market
Stanford HAI – AI Index 2026, Economy: https://hai.stanford.edu/ai-index/2026-ai-index-report/economy
Lightcast – Stanford AI Index 2026: https://lightcast.io/resources/research/stanford-ai-index-2026
Eurostat – Use of AI in enterprises (Dec. 2025): https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20251211-2
Eurostat – Digitalisation in Europe 2026: https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2026
UC Today – Gartner forecast on AI agents: https://uctoday.com/gartner-predicts-40-of-enterprise-apps-will-feature-ai-agents-by-2026

BNB markets

BNB Markets supports high-tech, electronics, and semiconductor companies with outsourced B2B marketing services. We conduct market research, benchmarking on technology or product and market-oriented strategies, marketing automation, and content marketing. We also engage in relational marketing, such as researching information on exhibitions or organizing targeted conferences. BNB Markets collaborates with various entities in the industrial, space, and medical sectors.

© BLACKNBLUE MARKETS 2026