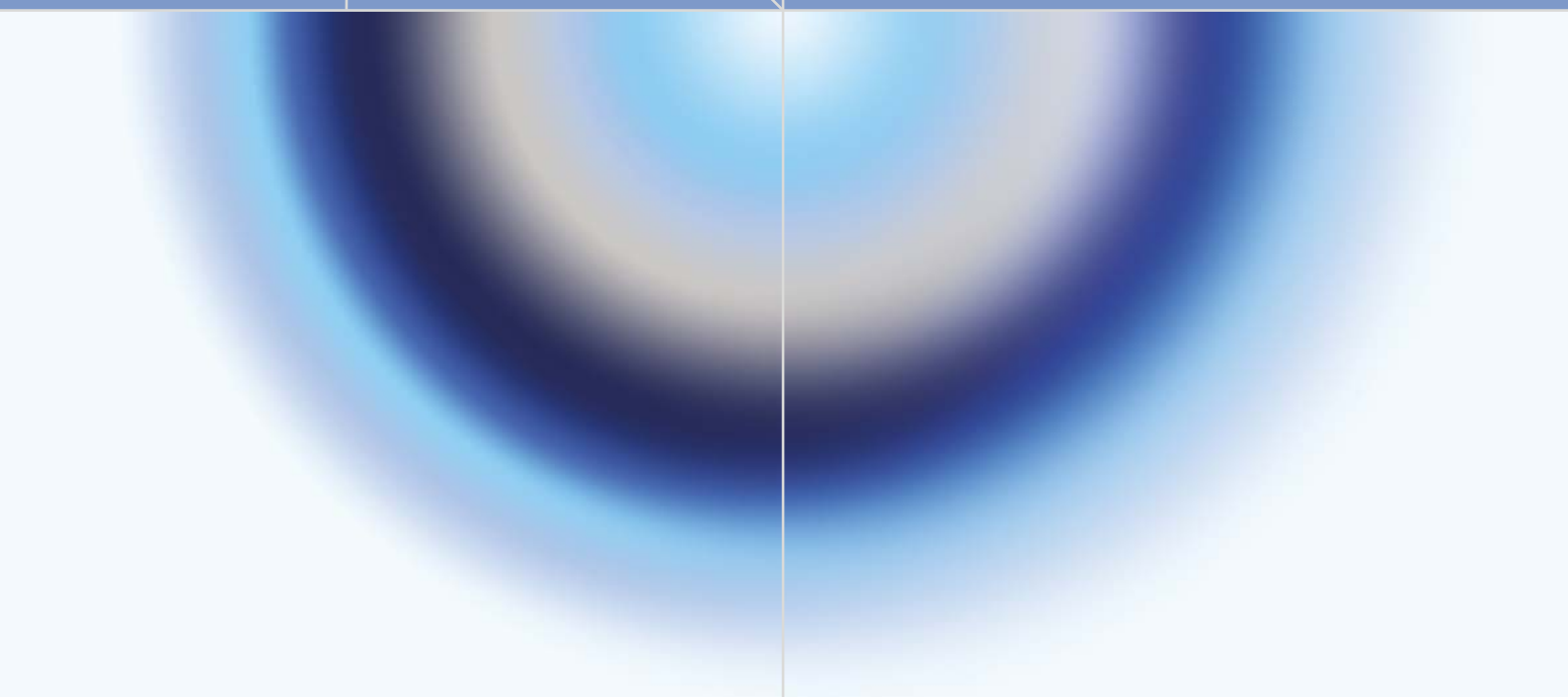
Intelligent Industry

IQ

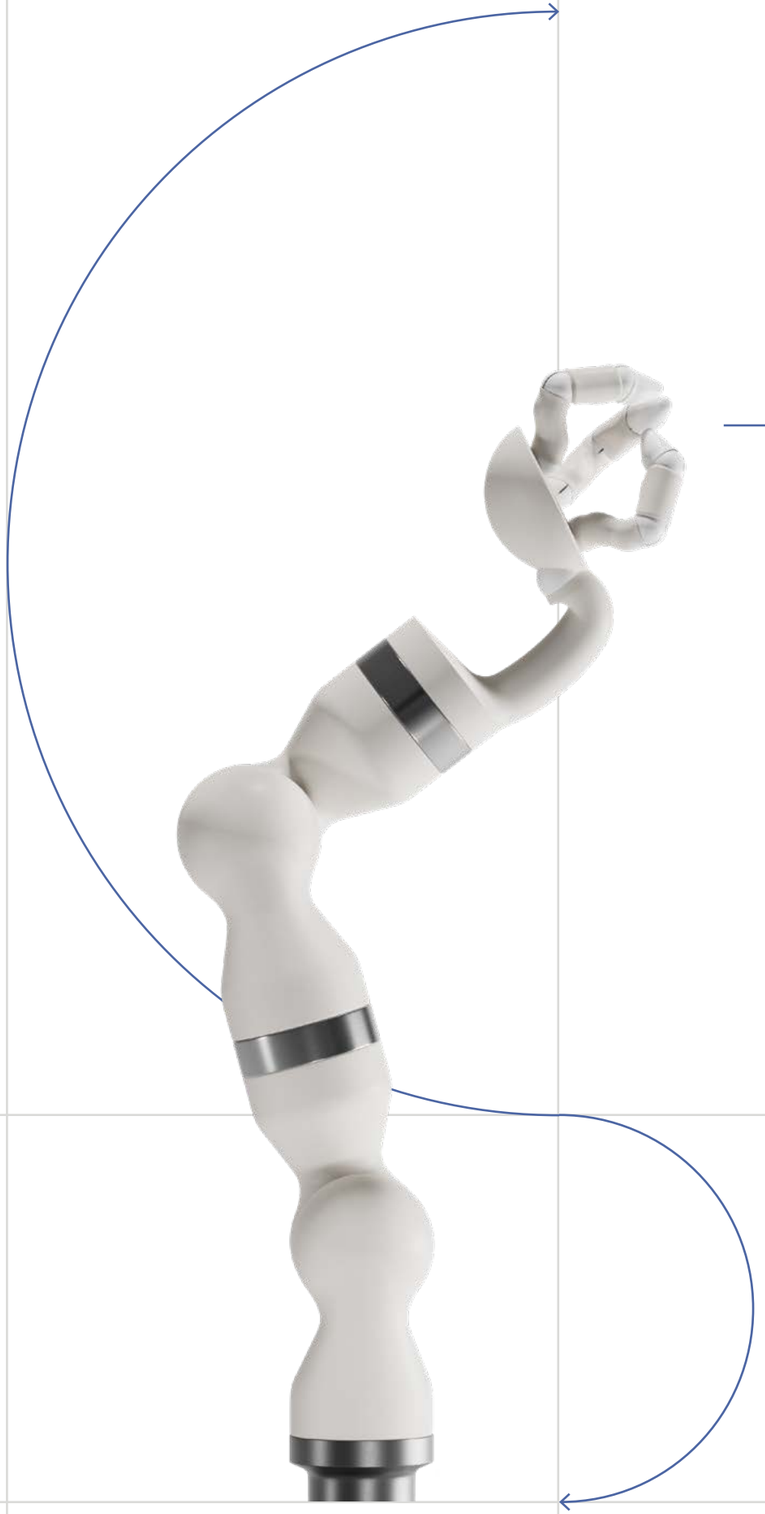
More than the sum of its parts.
Assembling new capabilities for industrial business intelligence.



Issue #01

IBM

IQ



Introducing, industrial-grade digital solutions for tomorrow's leading manufacturers.

Intelligent
In*d*ustry

Automotive

Aerospace & Defense

There’s no time like tomorrow in the manufacturing sector. Generative AI is here and quickly transforming the way we think about business intelligence. Software-defined products are driving a shift in workforce skills and human potential is being augmented with data and transparency across global operations.

IQ Magazine is an exploration of today’s technologies that are converging to create a more intelligent future. One where manufacturers confidently harness the digital revolution that’s knocking on our door.

This magazine series is part of Intelligent Industry, IBM Consulting’s initiative to inspire digital transformation in the manufacturing industry. We’re proud to share our wealth of knowledge and inspiring content with our partners and clients—past, present and future.

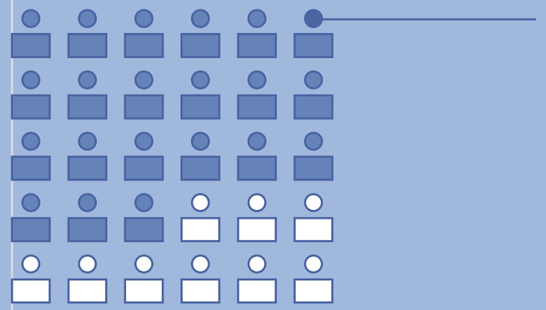
Thank you to our readers and contributors who made this inaugural issue possible.

Industrial Manufacturing

Industrial Service

AI makes way for a new day-to-day

Generative AI's highest value impact culminates in best-in-class experiences that re-calibrate what's possible for employees and customers.



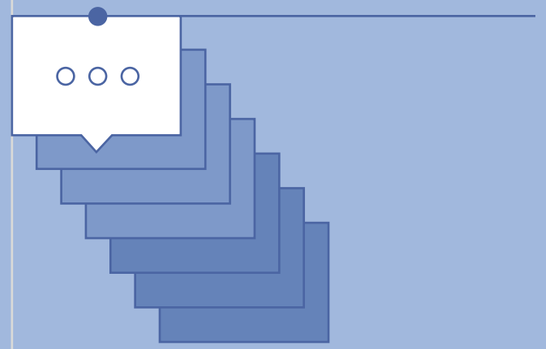
Nearly **70%** of entry-level manufacturing jobs are expected to be transformed by 2025.

To change the way people work, investing in AI enabled platforms is the top priority.

Industrial executives expect available AI-implementation budgets to grow to more than double last year's levels.

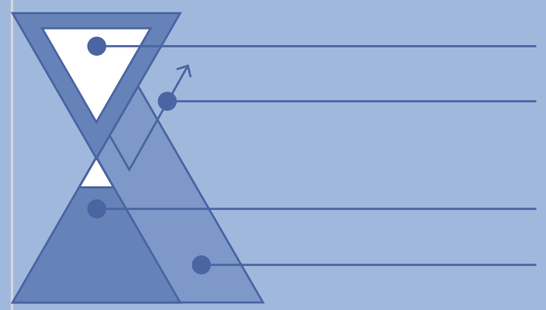
Platforms show new promise

Generative AI is creating leaps in capability with increasingly intuitive functions that virtually all businesses can take advantage of anywhere humans, data, and information meet.



Platform initiatives include:

- Field Service
- Customer Relationship Management
- Self-serve Catalogues
- Product R&D
- Quality Assurance
- Talent Development



In the past, as much as **83%** of platform-based transformations have failed.

Executives see Generative AI as the missing link to ensure success.

New platforms are now on the table for **91%** of industrial CEOs.

An increase of **49%** since 2018.

Tomorrow's leaders need IBM today

Marcus Claus
Partner
Discrete Manufacturing Lead | DACH Region

Let's connect on LinkedIn

To our esteemed readers and valued clients,

I'm thrilled to share the first edition of IQ, a magazine dedicated to providing you with the latest insights, trends, and thought leadership in the world of discrete manufacturing, encompassing Automotive, Aerospace & Defense, Industrial Manufacturing, and Industrial Service industries.

As we navigate a rapidly evolving landscape of digital transformation, it's my personal commitment and that of IBM Consulting's, alongside my Discrete Manufacturing team, to be your most valuable transformation partner and industry consultant. Our mission is to support you in overcoming industry-specific challenges and empower you with reliable, future-ready solutions that drive growth and innovation in your business.

Our multifaceted expertise combines a deep understanding of discrete manufacturing industries with our holistic approach to strategic business and IT consulting, process consulting, implementation consulting, hybrid cloud solutions, and application management support, to consistently deliver powerful tailored solutions for the unique needs of manufacturers around the world and in the DACH region.

Looking ahead, we see a new wave of business and product innovation driven by generative AI, and with it, a more capable and agile manufacturing industry. As we explore the importance of AI in this issue, IBM Consulting's unwavering dedication to implementing AI-driven platforms that are transparent, trusted, and fair is essential.

We know successful digital products and platforms can only create value for everyone involved when AI ethics and data governance are in focus at the highest levels of your organization. And as industry leaders, and trusted partners, it's up to us to steer the impact of the enterprise AI revolution.

As we embark on this transformative journey together, I want to reiterate our commitment and, with confidence, assure that your future will be a more intelligent one.

Best regards,
Marcus

"It's up to us to steer the impact of the enterprise AI revolution."

Assembling an ecosystem

To begin modernizing supply chains and extracting the full potential of networked technologies, companies must start with strong digital infrastructure that delivers real-time access to data across an enterprise and its collaboration partners.

The digital components for a supply chain that thinks.

Downtime can be costly. And in increasingly complex networks, modern supply chains need to predict the future, create visibility with ease, and react in real-time.

Today, speed and reliability are among the top benefits seen by companies leading the charge in intelligent supply chain transformation. But relentless innovation in AI-managed and integrated platforms are uncovering new opportunities for revolution in demand forecasting, supplier collaboration and service delivery to name a few.

Manufacturers need to react quickly as more clients expect configure-to-order, make-to-order and make-to-stock products. To manage more complex product and service offerings, companies need intelligent systems to manage these orders and overcome the effort needed to create data transparency across legacy systems in an increasingly complex market.

1. Intelligence:

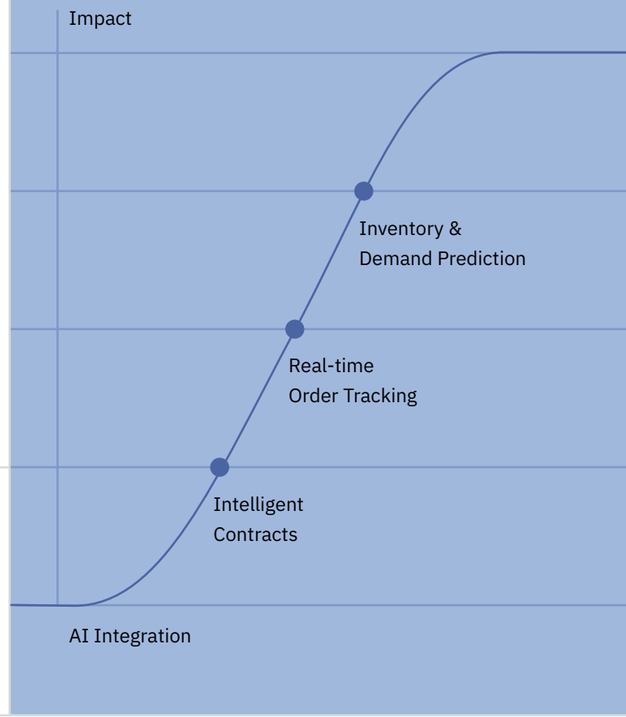
AI Augmented Digital Platforms and Predictive Analytics

Insight
By using AI and predictive analytics, companies can transform their supply chains into intelligent systems that can predict and avoid future problems. AI-powered platforms can identify risks, react to developing supply events and improve the quality and yield of operations.

Action
Implement AI-powered platforms to connect participants, collect real-time data, and enable continuous learning. Use predictive analytics to improve demand planning and forecasting. Robust-but-flexible data architectures with intuitive user interfaces let companies respond to new market dynamics, customer demands, and user needs.

Outcome
Improved supply-chain visibility and coordination enables organizations to deliver projects on time and at a lower cost. Companies that have adopted digital supply-chain strategies have seen improvements in supply chain efficiency and effectiveness.

Companies ahead of the curve are seeing the biggest results by implementing AI-enabled processes in some of their most important operations.



2. Efficiency:

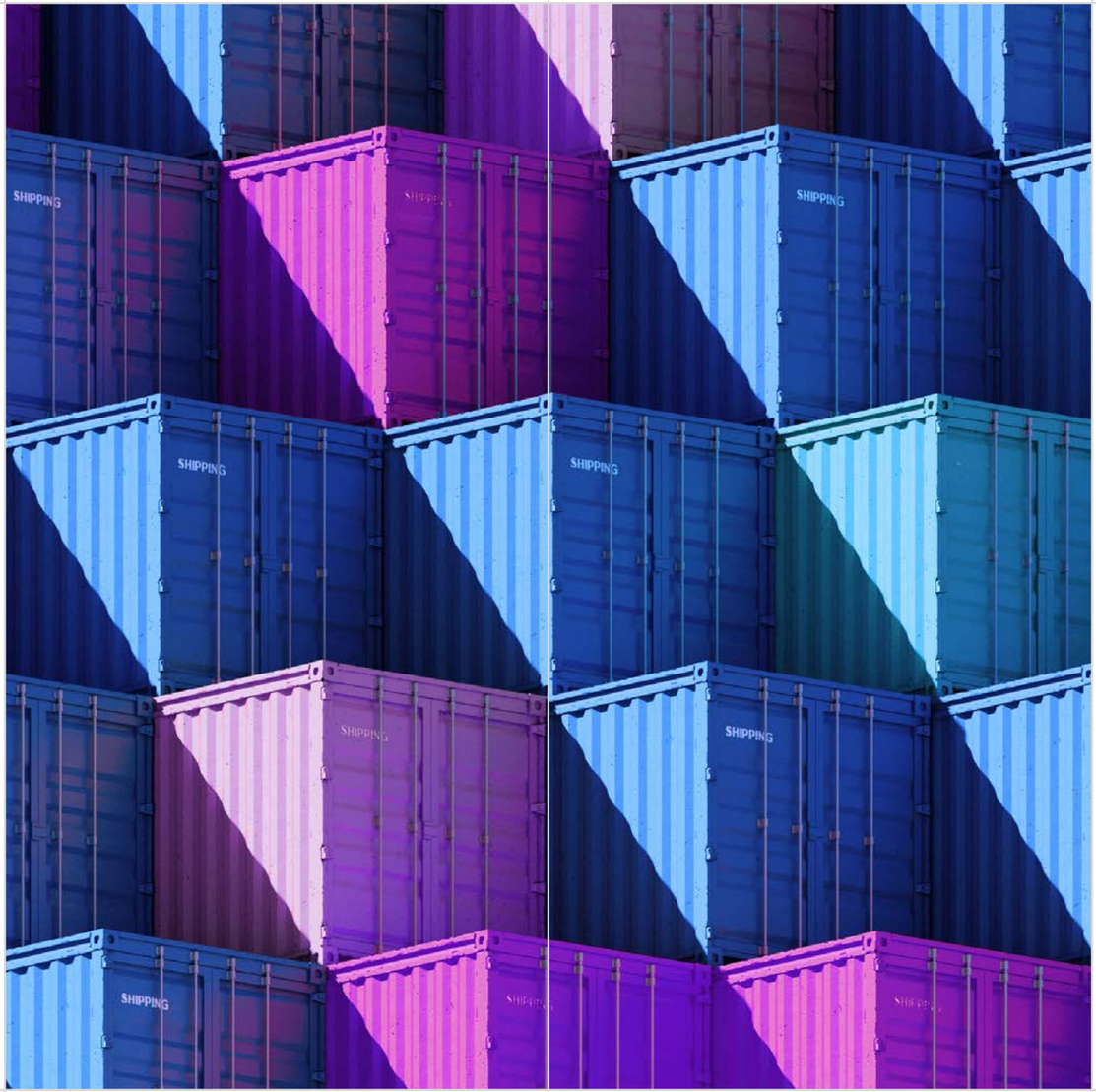
Automation and Internet of Things (IoT)

Insight
The integration of IoT and automation technologies can help supply chains become more efficient by improving reliability, performance, and resource consumption. IoT devices can provide connections across ecosystems, while automation systems can help manage assets and improve operational efficiency.

Action
Implement IoT devices and automation systems to connect ecosystems, manage assets, and improve operational efficiency. Use these technologies to synchronize schedules across internal and external parties and maintain control over materials, equipment, and supplier milestones. Synchronized schedules help supply-chain changes propagate across a schedule hierarchy by adjusting forecasts, procurement, and delivery. Value-chain visibility helps maintain control of intelligent IoT assets that use cognitive insights to improve performance.

Outcome
Reduced downtime, lower costs, reduced waste, and improved resource use lead to a more efficient and agile supply chain. Manufacturers that have embraced these technologies have seen improvements in productivity, cost structure, and resource consumption efficiency.

Reduce time-to-value by as much as **85%** with AI-powered B2B networks that can retrieve order and transactional data up to **90%** faster.



“A digital supply chain is a competitive advantage. Systems that support integrated planning, value-chain visibility, and intelligent assets, address the large effectiveness gaps in typical supply-chain networks.”

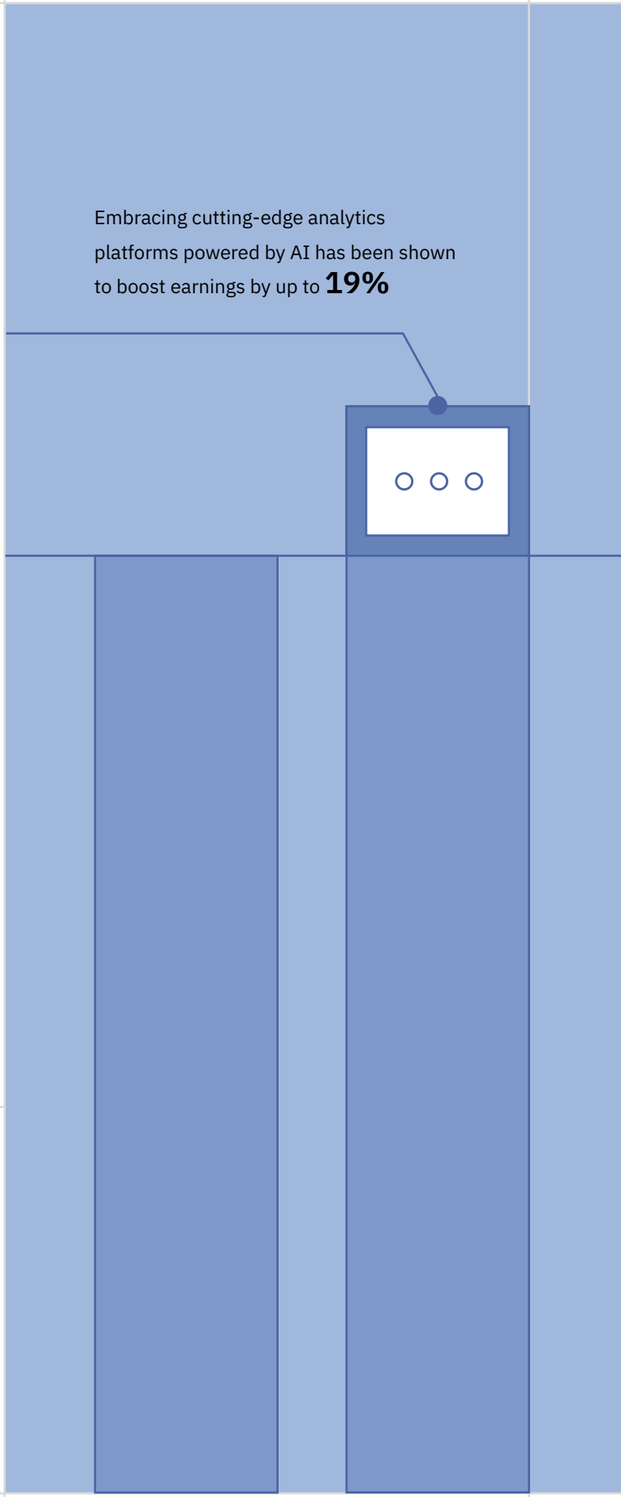
3. Profitability:

Financial, Sales, and Operations Planning

Insight
By digitizing financial, sales, and operations planning, companies can gain greater control over their supply chains, leading to increased profitability. Digital platforms can connect companies with customers and partners to share supply-chain information and conduct transactions, resulting in increased revenue and decreased infrastructure costs.

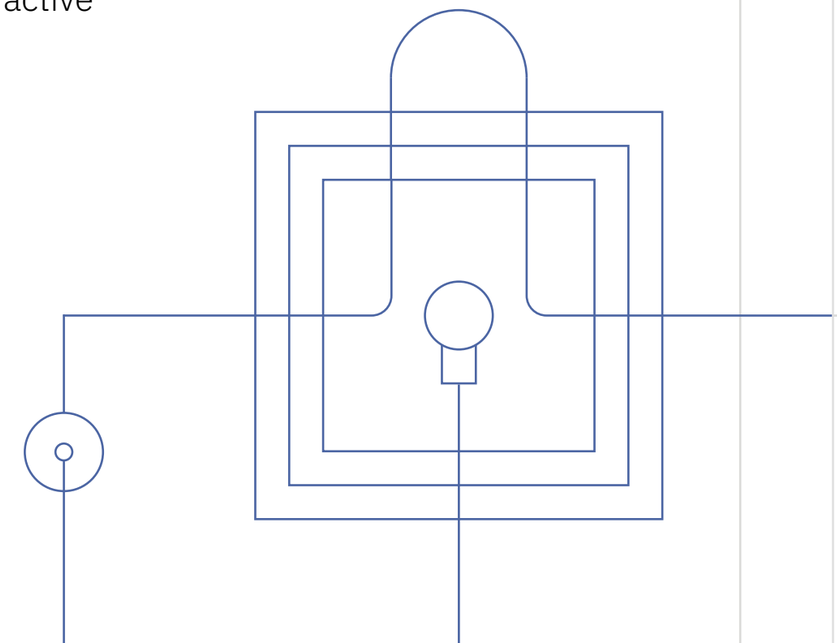
Action
Use digital platforms to share supply-chain information and easily process transactions with customers and partners. Integrate data from various sources to improve supply-chain performance and predict demand, enhancing sourcing and decision-making. Leaders in digital supply chain management have invested heavily in cloud computing, predictive analytics, IoT, and AI technologies to improve sourcing, supplier management, demand planning, forecasting, and asset management.

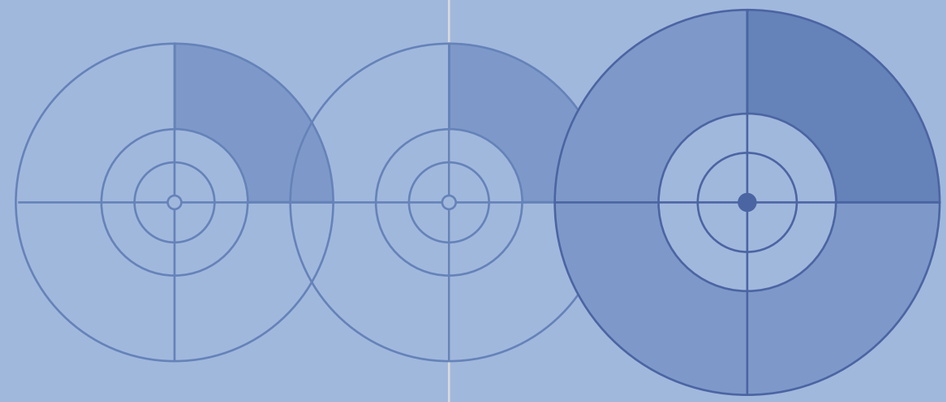
Outcome
Increased revenue, decreased infrastructure costs, and improved operational efficiency all lead to a more profitable and sustainable supply chain. Companies that have successfully digitized their supply chains have experienced improved financial performance and a greater ability to address supply-chain and market challenges.



Keeping pace with intelligent threats

The potential to create real-world damage makes the manufacturing industry particularly attractive to cybercriminals.





In 2023, **25.7%** of all cyberattacks were in manufacturing, continuing the sector's three-year run as the most attacked of the top ten industries globally.*

"I believe it's a combination of factors that make the manufacturing and automotive sector especially attractive to attackers. Many large Automotive and Industrial businesses do have dependencies on a network of multiple suppliers. A successful disruption through a cyberattack on a single medium sized manufacturing company can result in huge damage to the business. So, there is a lot at stake if a single business is targeted by ransomware attacks—whether a company has an outage, whether they lose sensitive data—what's at stake can be as important as the ability to produce and do business", says Kevin Euler, Associate Partner with IBM Cybersecurity Services.

Despite cyberattack trends outside manufacturing showing data theft and leakage incidents becoming the most common impact for organizations, increasing 32% year over year, ransomware still holds outsized relevance in industrial sectors.*

Few industries have the same severe consequences from a cyberattack as manufacturing. Today, theft of sensitive or secret information in the form of patents, credentials and personnel details poses a clear danger to organizations and nations. This comes often with the fact that A&D supply and value chains are fragmented and often decentralized locally due to industrial policy. And many leading manufacturers in other areas are innovating at a pace where vulnerabilities in the digital integration of production machinery or physical end products might soon lead to physical harm to people or industrial assets and environments.

In a business era defined by a push toward interconnected systems where operational and information technology meet, the manufacturing industry finds itself in the crosshairs of threat actors who are constantly adapting and refining their techniques. They are able to leverage more access points with each new digital interface workers and users interact with on a day-to-day basis.

Many small and medium-sized businesses that are intimately intertwined with larger supply chains may not be as well-protected from an attack compared to their larger enterprise cohorts. And that makes them an appealing victim for attackers because it's comparatively easier to enter their systems. Once they're in, attackers may find more opportunities for disruption, destruction and ultimately extortion if a threat cannot be contained to a single system—a common response method used by well-prepared organizations.

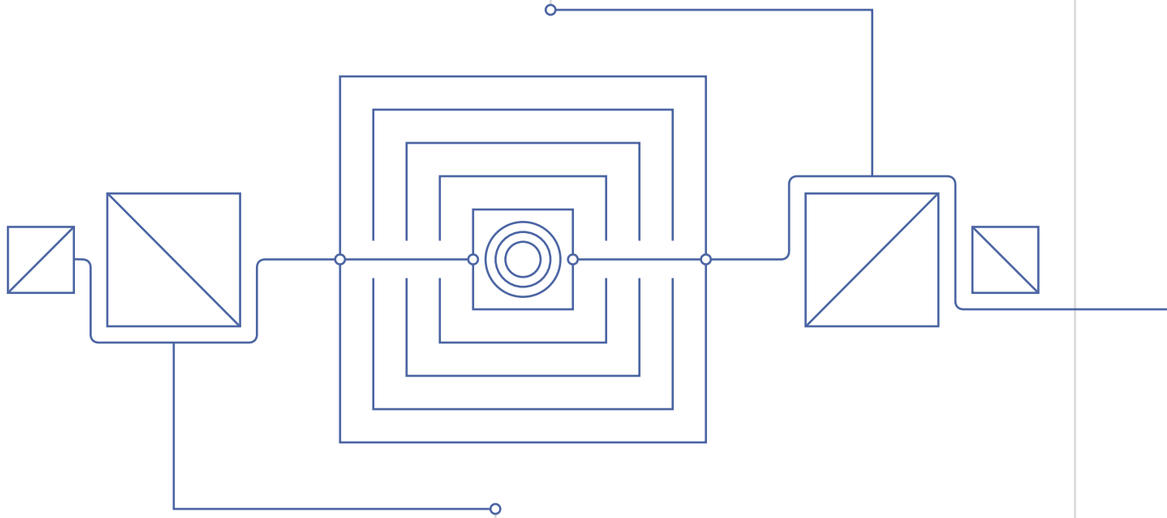
"For a long time, the industrial manufacturing sector has not been as regulated as, for example, the banking and insurance sectors which have very strict mandatory regulations from authorities in place. There have been almost no comparable regulations for many manufacturing sectors [...] and that's of course known to the attackers", says Euler.

There are some signs showing that security awareness and development are normalizing. Once only in the realm of large global enterprises, security operations are now a standard part of many businesses inside and outside of the manufacturing sector. Furthermore, organizational and governance structures reflect this progress.

Today, CISOs (Chief Information Security Officer) hold more prominence than ever—a role that only 5 years ago didn't exist much outside of technology firms—and their trusted security experts are shifting from security system operators to integrated roles in application development teams.

"You need to think about security from the very beginning—when you develop the product, when you develop the application", says Euler, adding, "I believe the right approach is to keep pace and to make sure security is at a constant high level. Even though there are more and more interfaces, more and more applications, more and more automation in, and connected with, physical products and devices."

But keeping pace, as Euler describes it, is not just about matching evolving cyberattack capabilities. As manufacturers' own product and service innovations gain new software-enabled advantages and empower end users in more ways than ever before, they're also creating more inroads for attackers to exploit.



"You need to think about security from the very beginning—when you develop the product, when you develop the application."

Everything from a digital twin software for product design to in-field technician applications that support after-sales service, and even user interfaces on a software-enabled home appliance can be a new attack vector in the form of another user-login modal.

One of the top initial access vectors in 2023 was the abuse of valid user accounts, accounting for 30% of incidents. Organizations' increasing reliance on cloud-based interfaces for day-to-day operations and product functionality is putting a large portion of the responsibility of secure access on an end user who's saddled with more and more personal credentials to manage. And these account credentials are steadily becoming more available for purchase on the dark web, making it easy for attackers to take over legitimate user identities and establish access.*

**Article data and insights from 'X-Force Threat Intelligence Index 2024' IBM X-Force is a threat-centric team of hackers, responders, researchers, and analysts.*

A comprehensive security strategy that employs zero-trust, as well as identity and access management practices, like multi-factor authentication and routine credential audits can be a vital defense against unauthorized access. Although, defending against an attack is only half the battle. In addition to continuous monitoring and threat intelligence, network segmentation can effectively isolate critical systems and limit the lateral movement of attackers within a network.

And as we see cyber attackers edge closer to more complex and powerful attacks that leverage AI, or simply lagging security practices, manufacturers will be forced to adapt. Suppliers, OEMs and industry associations will demand that smaller manufacturers consider security principles in the development of their products. Whether in new product segments or established supply partnerships, proactive security practices will become an important relationship factor and may lock out manufacturers who don't adapt.

Waiting for Day Zero

The malicious side of AI breakthroughs that can’t be ignored.

A Zero Day attack is defined as a cyberattack or threat that has never been seen before. It presents a completely novel threat and tests even the most advanced cybersecurity infrastructure. Today, Zero Day vulnerabilities make up a very small percentage of attacks—currently at only 3%—and in 2023, that amounts to a 72% drop compared to 2022.*

It's natural to imagine AI becoming the most powerful and easily deployable cyberattack mechanism we've ever seen. And certainly, cybersecurity experts are thinking the same. But the reality isn't so bleak. At least not yet.

"Is this already happening? No. I would say there are examples, but it's not a major attack pattern that's happening right now. In my opinion, because the effort is still quite high and there are easier ways [...] but as companies are preparing more and more against traditional threats, it is becoming more important very very fast. And companies have to start preparing IoT security against these types of threats now", says Kevin Euler, about the prevalence of both AI-enabled cyberattacks and cyberattacks targeting AI-enabled systems or models.

However, some assessments see AI as a fast-growing catalyst for a new wave of powerful, unfamiliar attacks. Today, generative AI models are used to exponentially increase an individual or group's capacity to perform phishing campaigns, crafting content made to deceive, and perform other malicious communications.

Trends show that the same push for the development and maturity in enterprise-grade AI solutions is also fuelling an AI maturity race for cybercriminals. In fact, it's been reported that 'AI' and 'GPT' were mentioned in over 800,000 posts on illicit markets and dark web forums in 2023.*

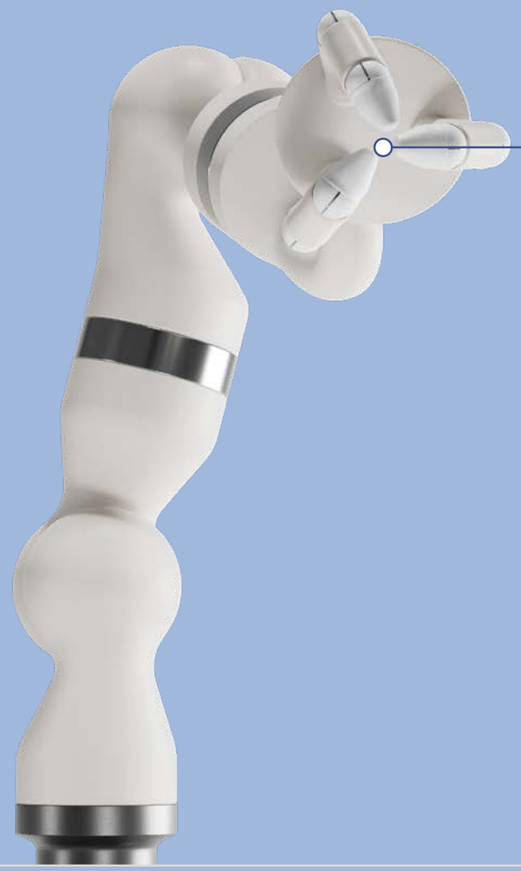
Despite this interest, some signs indicate that until a high-enough marketshare is reached by a few dominant consumer-side LLMs, the investment required for attackers to develop truly intelligent AI threats is too great. But as we all know, with AI change can happen in an instant and it might not be long until we're defending against malicious LLMs with names like WormGPT or FraudGPT.

**Article data and insights from 'X-Force Threat Intelligence Index 2024' IBM X-Force is a threat-centric team of hackers, responders, researchers, and analysts.*

Go beyond human capability

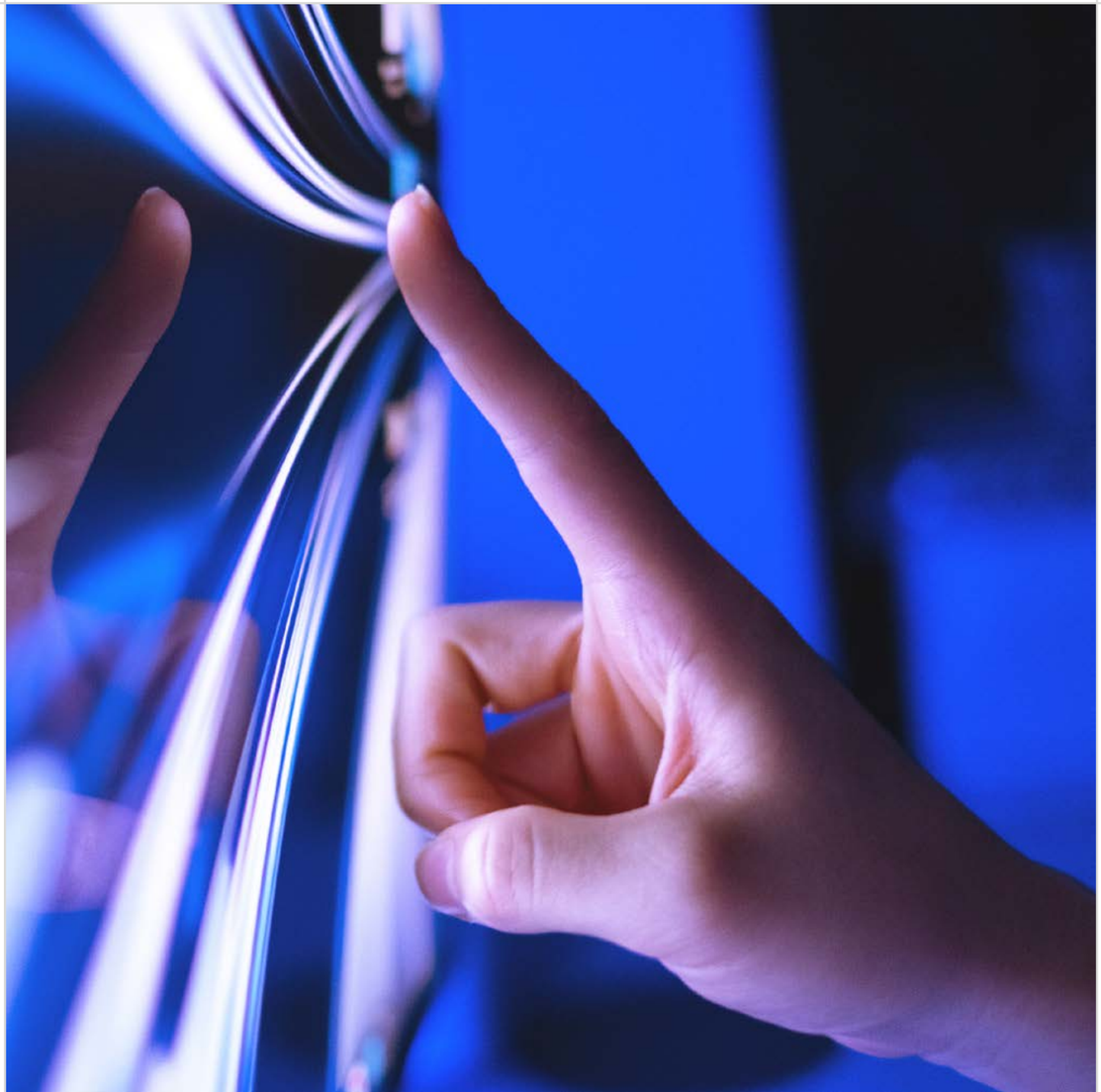
Intelligence that turns data into insight. Automations that turn insight into action.

Meet the next generation of production.



IBM

Symbiotic relationship



Human intelligence augments advancements in AI-enabled automation.

Exponential adoption of industrial robotics in the past decade has exemplified the automotive industry's appetite for increased automation on factory floors. But as advancements in AI create new potential, it's crucial to recognize the indispensable role human workers will continue to play in an AI-enabled industrial future.

It might be tempting to extrapolate from current trends in automation and assume that a "lights out" factory is both a near and direct path to the utmost efficiency, but some automakers chasing that fully automated future have discovered something surprising.

Even with highly capable generative AI systems, human adaptability and judgment in unexpected challenges are still required to handle complex tasks. Certain manufacturing tasks, even when automated, require real-time problem-solving that cannot be effectively executed by robots alone.

Ford's truck plant in Kentucky echoes this sentiment. Here executives have stressed the indispensability of human ingenuity in keeping the production line not only running smoothly but constantly improving. Once a process is automated, the efficiency improvement becomes stagnant. Only human interaction with the tools and processes can uncover new opportunities in established workflows and processes.

Product innovations in electrification and software-intensive vehicles are driving a seismic shift toward digital complexity and novel manufacturing processes. This shift necessitates a workforce with new skillsets in robotics orchestration, additive manufacturing or IoT (Internet of Things) system architecture, to name a few. Even with AI set to drive up efficiencies within these new skillsets, the automotive industry's need for continuous productivity improvement necessitates a fresh approach to reskilling. An approach that safeguards valuable institutional knowledge as the pace of technological change renders certain worker skills obsolete.

The challenges of attracting new talent and the impending retirement of technical experts pose additional hurdles. Reskilling employees—on which the automotive industry is projected to spend billions of dollars over the next decade—and investing in continuous learning platforms are essential to keep up with evolving technologies.

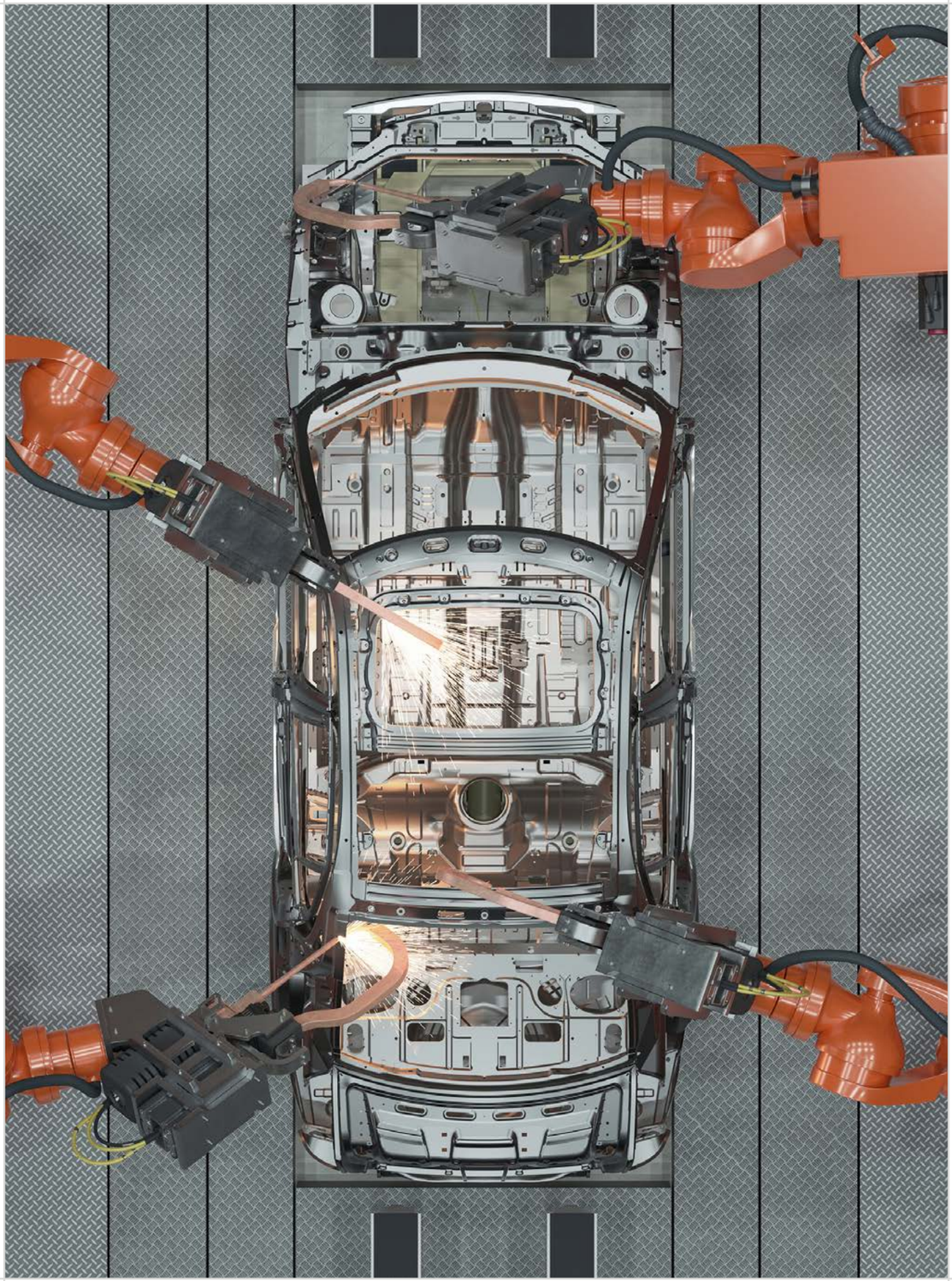
One major European OEM has already embraced AI to build the right human capital for its organization. With AI digital assistants, candidates are guided through the application process in a user-friendly manner, while recruiters gain a comprehensive view of skills and recruitment data. This innovative approach not only streamlines the hiring process but also ensures that the right talent is acquired to drive innovation and growth.

While reskilling and acquiring new talent are imperative, it is equally important to empower workers with the right digital tools and AI assistants. In today's manufacturing plants, workers often struggle with information overload or a lack of essential information to solve problems effectively. Empowering them with AI-enabled tools integrated into their workflow can significantly enhance their capabilities and improve productivity.

For instance, some industry technology leaders believe that providing line operators with additional digital work instructions, process explanations, and voice-enabled manuals can greatly benefit their performance. However, it's important to remember that implementing digital tools, including AI, is most effective when the user is at the heart of the digital product design. This ensures worker-facing tools have intuitive digital interfaces and app-like functionalities.

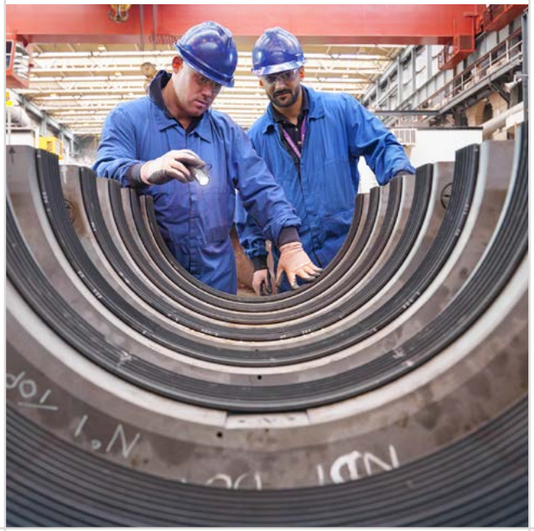
Augmented Reality (AR) is already being explored to augment even very human-reliant manufacturing tasks like quality inspection. AR hardware and software products can let technicians, inspectors, and engineers identify and share defects accurately, integrating real-world data and imagery with advanced virtual vehicle models. This technology has the potential to streamline responses, reduce errors, and enhance collaboration, ultimately improving the overall productivity of every essential human worker in that process.

Once a process is automated, the efficiency improvement becomes stagnant. And only human interaction with the tools and processes can uncover new needs and opportunities in established workflows and processes.



Beyond productivity, AI tools can also play a crucial role in keeping employees safe in manufacturing environments and reducing health and safety incidents. An AI-enabled visual inspection system can monitor the proper use of personal protective equipment, or scan environmental conditions or assemblies for risk factors. Virtual assistants that can provide real-time information on procedures, risks, and support for critical situations can help employees navigate the workplace safely and with more knowledge at their fingertips.

It's essential to recognize that the human element remains at the heart of manufacturing. Skilled workers bring a wealth of experience, adaptability, and problem-solving capabilities that are difficult to replicate in AI systems. As the automotive industry and other industrial sectors embrace AI and advanced robotics, the focus must now shift towards augmenting human capacity rather than replacing it. Whether it's to enhance workers' capabilities, streamline processes, or create safer work environments, the people remain at the center of the value proposition for these new technologies.

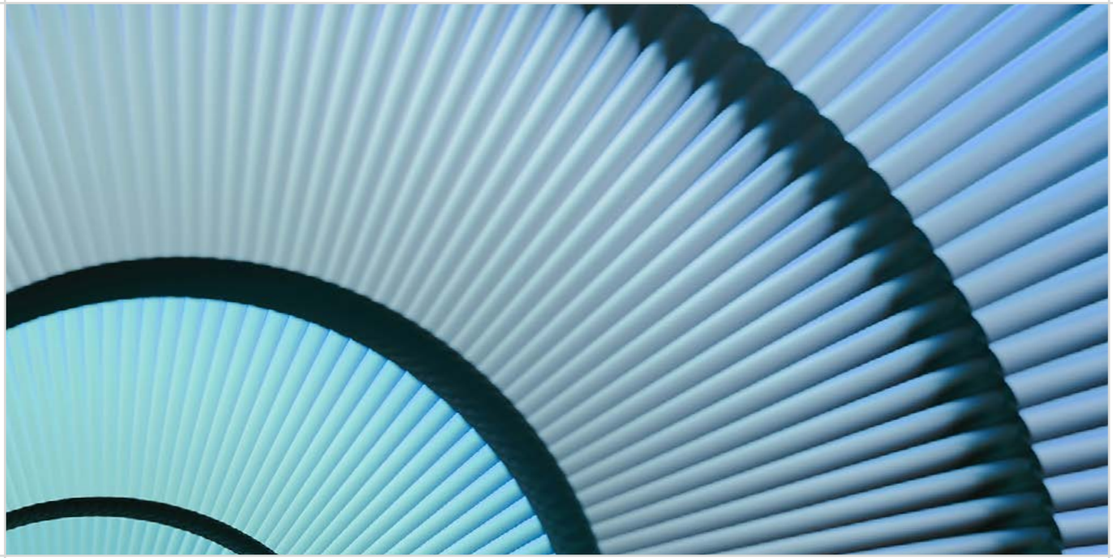


It's important to remember that implementing digital tools, including AI, is most effective when the user is at the heart of the digital product design to deliver the ease and functionality of the personal devices and intuitive digital experiences they're already familiar with.

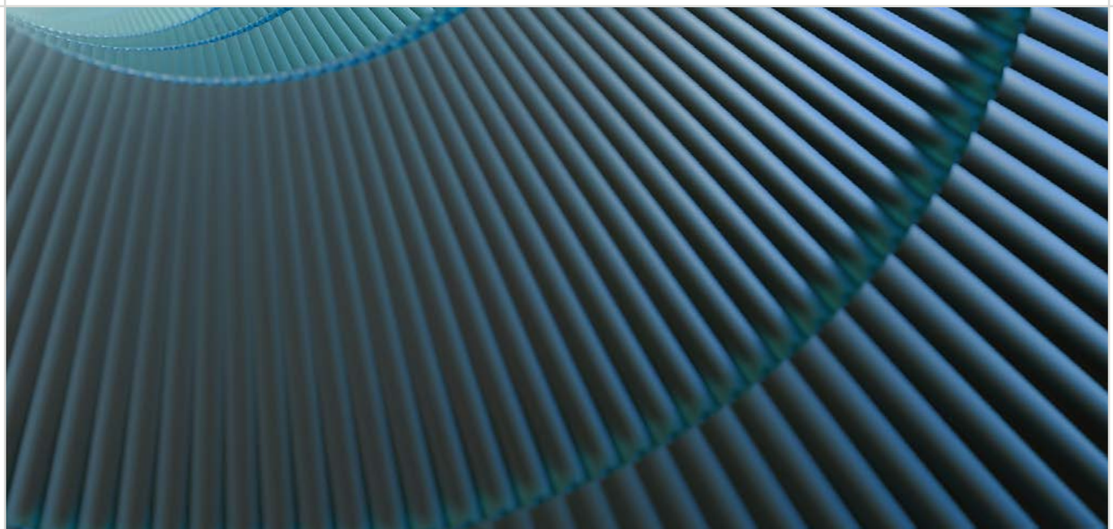
Let’s create → tech stacks that enable visions

Learn how we can help your business harness complex data streams with Hybrind Cloud at ibm.com/consulting

IBM



Critical agility



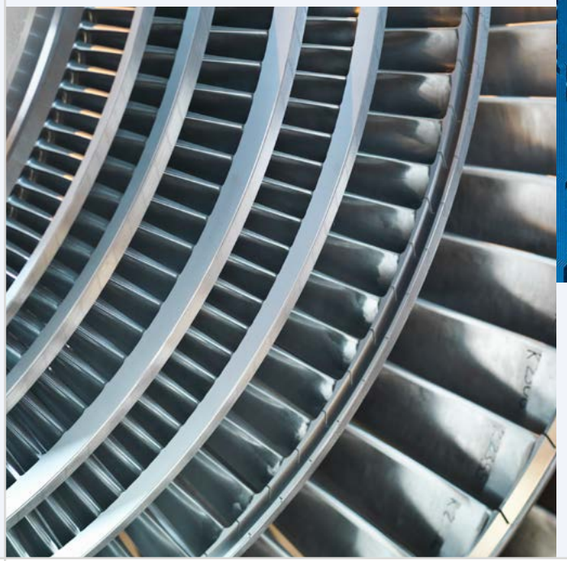
How software and AI will accelerate innovation in defense organizations.

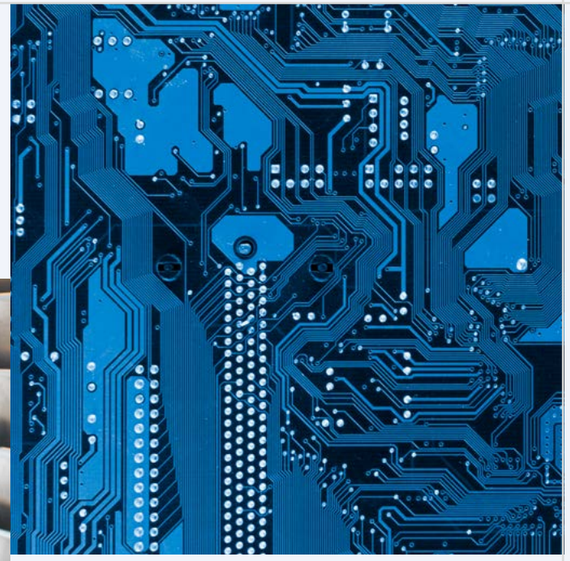
Rapid innovation cycles that bring new capabilities and features are the norm for everyday consumer technology platforms. This is far from true for military platforms. A much-needed paradigm shift is under way.

Until recently, a vast majority of military platforms, i.e. airplanes, tanks etc..., went through long-term cycles of research, planning, concept development and procurement—each of which could take years, even decades between inception and platform delivery. This left many Ministries of Defense in a difficult situation, constrained by these prolonged cycles while, at the same time, pressured to accelerate their pace of innovation. Fortunately, more and more differentiating capabilities in defense are shifting to a new, software-defined paradigm, which, by its digital nature, requires immensly shorter production cycles.

Hence, the concept of “Software-defined Defense” is gaining traction in NATO countries and the greater defense industry. Broadly speaking, the vision for the procurement side is that new software-defined capabilities be made available in a much more rapid way, like on a smartphone. And it’s not just about speed, new capabilities might be sourced from a variety of partners, similarly to how applications are offered on a certified open marketplace that is established by a smartphone platform provider.

This concept presents a radical shift that plays out in the technical, procurement, contractual and organisational spaces. It also introduces challenges for the business models of the established military platform providers.





Continuous updates via support and maintenance contracts have already been put in place. However, experience from the conflict in Ukraine has demonstrated a radically different approach to quickly developing and deploying new capabilities in the field. This is what ministries of defense are studying and trying to learn from.

It's been observed that relevant innovation can come from many parties and that often new ways are found to equip legacy platforms with as yet unforeseen technology. Hence, defense organizations are building up their own AI- and software development capabilities and engaging in an active dialogue with the ecosystems of partners, both traditional and new.

The industry is ready to engage, but there are challenges yet to be solved. They are addressed on a conceptual and implementation level. One example is the German task force that develops concepts for software-defined defense under the umbrella of the BDSV.

Moreover, defense organizations have begun to build or are already providing platforms for software development and distribution. Examples include the DevSecOps Software Factory Platform One by the US Department of Defense and the D2S platform of the UK Ministry of Defense. Open technology and open standards are an important building block for these platforms.

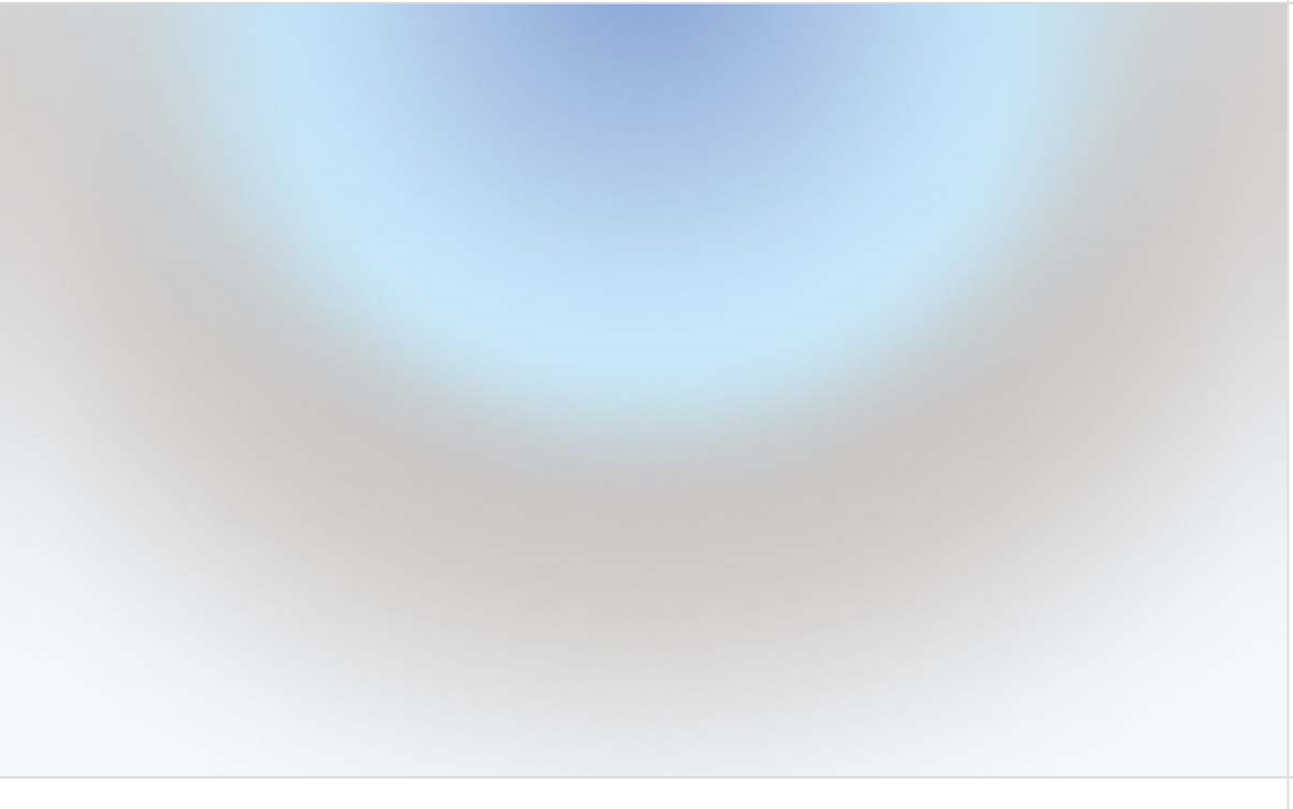
Artificial intelligence (AI) can benefit from these DevSecOps platforms, but the development and responsible use of AI requires more. It is without question that the use of AI has to conform with the ethical norms of our Western societies. Furthermore, it must abide by humanitarian law. Standards have to be developed for a comprehensive quality management of AI solutions. This requires, among other things, a comprehensive documentation of the AI solution, starting with details on the use case, training data, training code, model code as well as test and certification results. We have to keep track of what update has been supplied to what device. And the number of these devices (e.g. several swarms of drones) could run into the thousands. While in use, performance of the model has to be monitored, feedback has to be collected and updates have to go through the whole quality management and deployment cycle.

This kind of comprehensive management is impossible without a system such as a Machine Learning Ops (MLOps) platform. Skilled personnel, essential for building and implementing such a system, are scarce in militaries. A 2022 report from the US National Security Commission on AI identifies this skills shortage as the single greatest inhibitor to buying, building, and fielding AI-enabled technologies for national security purposes.

The demand for, and scarcity of, these skills presents a great opportunity for collaboration—to build platforms for data and AI and to co-develop trustworthy AI solutions. But there's not only this need for AI—AI itself is now mature enough to accelerate SecDevOps and the development of new AI solutions. The war in Ukraine has shaken up Europe and the NATO countries. The time has come to act and to build on solutions and trusted platforms that are already available.

Dr. Stefan Mück *is a Partner and IBM Distinguished Engineer. He led numerous lighthouse projects with a focus on data- and AI-driven transformation within IBM. Within the BDSV he leads the working group on AI for Software Defined Defense and is a member of the AI and Ethics task force.*

The demand for, and scarcity of, AI skills presents a great opportunity for collaboration—to build platforms for data and AI and to co-develop trustworthy AI solutions.



IBM Consulting DACH
Discrete Manufacturing Industries Team

Marcus Claus
Partner
Discrete Manufacturing Lead | DACH-Region
marcus.claus@de.ibm.com

Ralf Zillmann
Associate Partner
Account Partner
rzillman@de.ibm.com

Karsten Nagel
Partner
Lead Account Partner
karsten.nagel@de.ibm.com

Tim Donnelly
Associate Partner
Account Partner
tim.donnelly@ibm.com

IO

Jochen Zipp
Senior Managing Consultant
Account Partner
jzipp@de.ibm.com

Michael Hellmann
Associate Partner
Global Center of Excellence for SAP Automotive
michael.hellmann@de.ibm.com

Kevin Euler
Associate Partner
Security Lead
kevin.euler@de.ibm.com

Yann Patrick Boehly
Associate Partner
Global Center of Excellence for SAP Aerospace & Defense
yann.boehly@de.ibm.com

© Copyright IBM Deutschland GmbH
IBM-Allee 1
71137 Ehningen, Germany

IBM, IBM Consulting, the IBM logo, ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at: ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

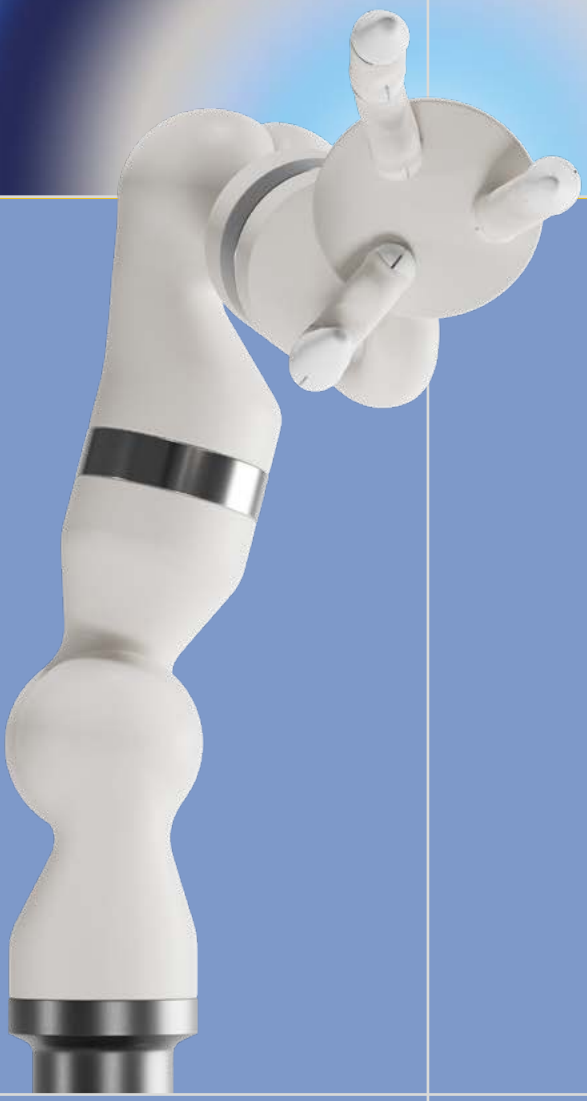
THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided. This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

Expert Insights represent the opinions of thought leaders on newsworthy business and related technology topics. They are based upon conversations with leading subject matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

The data used in this magazine may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an “as is” basis and IBM makes norepresentations or warranties, express or implied.

Intelligent Industry



IBM