In collaboration with Accenture

Intelligent Industrial Ecosystems: Turning Proximity into Intelligence

INSIGHT REPORT

AUGUST 2026

Images: Adobe Stock, Getty Images, Unsplash

Contents

Foreword

Roberto Bocca
Head, Centre for Energy and Materials, World Economic Forum

Miguel G. Torreira
Senior Managing Director, CEO Advisory, Commodity Markets Global Lead, Accenture

Intelligent infrastructure is changing how industrial systems are designed, optimized and operated across every sector, moving value creation from individual firm performance towards coordinated, system-level outcomes. This shift marks the emergence of the next frontier of industrial competitiveness.

This is especially pivotal for industrial clusters – geographical areas where companies and institutions operate in close proximity – and for industrial ecosystems more widely. The clusters that will lead in the next decade are those that combine the power of physical concentration with the intelligence that comes from data collaboration. As a result, energy systems, supply chains, logistics networks and resource flows can be optimized across the entire ecosystem, rather than on a company-by-company basis.

Trusted data collaboration makes this possible. When organizations share data securely and purposefully, they unlock outcomes that no single participant can achieve alone: energy optimization, system-wide resilience, circular resource flows and new commercial models built on collective visibility. Artificial intelligence (AI) amplifies this potential enormously, but only where the underlying data foundations are in place to support it. Without trusted, well-governed and interoperable data sharing across organizations, AI remains confined to isolated optimization, and the larger system-level opportunity goes unrealized.

This report addresses that gap, drawing from the World Economic Forum's Transitioning Industrial Clusters (TIC) initiative, the largest community of industrial zones in the world – with 42 clusters across 23 countries contributing approximately $900 billion to global gross domestic product (GDP). The report also builds on two Forum publications, *Five Steps for Digital Collaboration in Industrial Clusters*[1] and *Intelligent Infrastructure: A Primer*,[2] to argue that data collaboration is becoming a requirement for ecosystems seeking to remain competitive, resilient and investment-ready in the intelligent age.

The report offers a practical framework for moving from ambition to execution, grounded in value creation, trusted governance, data readiness, fit-for-purpose technology and cyber resilience by design. It draws on global implementation experience from leading industrial clusters across energy, ports, manufacturing and logistics.

Crucially, the governance models and collaboration approaches developed in cluster settings are not confined to them. Many of the lessons translate directly to broader industrial ecosystems, from national supply chains to cross-border industrial networks.

For business and public-sector leaders, the message is clear: the competitive advantage of clusters will increasingly depend on their ability to collaborate, not merely collocate. Those that begin now, with clear value cases and scalable models for collaboration, will be better placed to shape the next phase of industrial transformation.

Executive summary

Data collaboration is becoming the new frontier of industrial competitiveness, and those who build the foundations today will lead tomorrow.

Intelligent infrastructure is shifting value creation from individual firm performance towards coordinated, system-level outcomes where energy systems, supply chains, logistics networks and resource flows are optimized not company by company, but across the ecosystem as a whole. Evidence shows that data collaboration can unlock new system value.

At the Port of Rotterdam, the Starlings Project enabled industrial companies to trade energy flexibility in near real time across the cluster – something impossible without shared data. Early trials delivered efficiency gains of around 5%, but with more advanced data sharing, better system-wide optimization and improved platform capabilities, modelling shows that benefits could more than triple. Adding shared infrastructure could increase them even further, up to 8.5 times the original value. At the Ordos-Envision Net-Zero Industrial Park in China, shared data among more than 50 enterprises enabled coordinated energy optimization, achieving approximately 80% on-site green electricity consumption while reducing overall energy costs by around 10%. These are not isolated results – they reflect a pattern across ports, industrial parks and energy ecosystems worldwide.

However, most industrial ecosystems have made limited progress towards capturing this value. The barriers are mostly structural – spanning unclear value allocation, misaligned incentives, uneven digital maturity and cybersecurity exposures that grow with every new connection. If these barriers are not addressed, data collaboration cannot emerge and artificial intelligence's (AI) potential will remain confined to individual organizations.

Informed by over 60 senior executives and experts across consultations and global workshops, this report presents a practical framework to overcome those barriers and build trusted data collaboration. The framework has two integrated components:

1. Three stages guide ecosystems from intent to impact:
   - In the value case stage, organizations identify concrete use cases with clear system-level outcomes and build the business case for collaboration.
   - In the enablement stage, the data collaboration model is designed and implemented.
   - In the execution stage, use cases go live and the focus shifts to scaling and exploring new sources of value, such as adding participants, datasets and applications at a progressively lower marginal cost, creating the conditions for sustained innovation.
2. Four enabling foundations must be in place regardless of the collaboration model chosen:
   - Data governance establishes the institutional structures, decision rights and incentives that enable multi-party collaboration.
   - Data readiness provides a shared language that ensures data can be discovered, interpreted and trusted across different systems and standards.
   - Technology provides the architecture that embeds access controls, semantic alignment and policy enforcement into the infrastructure itself.
   - Cyber resilience protects the integrity of the whole system: in interconnected ecosystems, a weakness in one participant can propagate across the whole, and resilience must be built in from the outset.

Industrial ecosystems that invest in these foundations early reduce risk, but they also build the credibility that attracts partners, accelerates adoption and sustains participation over time.

> **The next frontier of industrial competitiveness lies in connected intelligent ecosystems: co-located organizations integrating data, infrastructure and processes across company and sectoral boundaries. This represents a profound shift from how industries have been organized for decades, but it's a necessary one if we are going to tackle higher-order business challenges. Innovators are already finding success with an approach I call 'radical collaboration', which prioritizes sharing insights with far-flung value chain partners, and even competitors, for mutual gain. That's the big leadership task ahead.**
>
> Caspar Herzberg, Chief Executive Officer, AVEVA

Introduction: Industrial ecosystems in the intelligent age

The clusters that will lead in the next decade are those that will be able to turn proximity into intelligence.

What stands out in this next era of record energy demand and artificial intelligence (AI) is the interdependence between energy sources and industrial outcomes – what we refer to as the Energy Equation. We must balance the outcomes society needs with the systems required to deliver them, and no single company, sector or nation can do it alone. Industrial clusters are where collaboration becomes practical; trusted data exchange enables us to deliver the system-level advancements we need.

Lorenzo Simonelli, Chairman and Chief Executive Officer, Baker Hughes

Countries around the world are facing mounting pressure to safeguard national industrial competitiveness amid intensifying geopolitical tensions, accelerating industrial transformation and the growing energy transition.

In this context, industrial clusters can play a central role in their national agendas by concentrating production capacity, infrastructure and expertise. They can attract capital for large industrial projects that create local economic development and jobs, help contain rising energy and material costs by developing shared energy infrastructure and improving resource efficiency, and facilitate innovation and technology transfer.

New technologies are becoming critical enablers for achieving such goals. Intelligent infrastructure is fundamentally changing how industrial systems can be designed, optimized and operated. A World Economic Forum's 2026 white paper, *Intelligent Infrastructure: A Primer*, shows that intelligent infrastructure integrates physical assets, data platforms and AI into coordinated "systems of systems" that can sense, learn and act in real time. At the cluster level, this enables a new class of outcomes: energy systems that balance supply and demand across multiple companies, supply chains that dynamically adapt to disruptions, and industrial companies that optimize resources collectively rather than individually.

Governments are increasingly recognizing this in their strategic industrial priorities. China, which has invested in industrial parks as a pillar of its industrial development strategy for decades, provides a notable example. In January 2026, China's Ministry of Industry and Information Technology and seven other central agencies issued a national AI and manufacturing action plan that ties cluster competitiveness to AI deployment, compute capacity, industrial datasets, application scenarios and benchmark firms, with explicit targets for 2027.[3]

Yet harnessing data to capture AI value remains a challenge, with only 32% of organizations saying they realize measurable value from data.[4] In industrial clusters, the challenge is even greater. The most valuable benefits emerge when operational, energy, logistics and environmental data can be securely combined across organizations. However, this often raises concerns about data sovereignty (the legal principle that information is subject to the laws of the country where it is physically stored or generated), cybersecurity, interoperability, governance and data sensitivity, thereby limiting progress in practice. Trusted data collaboration is key to unlocking AI-driven innovation and system value[5] creation, but it does not emerge automatically in clusters.

Clusters that fail to build the foundations for data-driven intelligent collaboration risk losing competitiveness, investment attractiveness, innovation capacity and resilience. This report outlines the main barriers to data collaboration in industrial ecosystems and shows how they can be overcome by establishing a data collaboration framework that provides a structured approach to scalable and secure value creation across the ecosystem.

While this report analyses industrial clusters, the principles of collaboration, data sharing and innovation discussed here equally apply to broader industrial ecosystems. Industrial clusters are a prime example of how collaboration encourages innovation. Yet, in an increasingly digital economy, ecosystems can form across geographic boundaries. Whether through shared data platforms, global supply chains or sector-wide sustainability initiatives, the patterns of trust, governance and value creation discussed in this report remain applicable.

> **Just as electricity once transformed how industries were built and run, AI is doing the same today – but on a foundation of data. Europe has a unique opportunity to become a global leader in industrial AI, building on decades of industrial know-how, engineering excellence and trusted industrial relationships. The companies and clusters that can connect data, technology and expertise across organizational boundaries will define the next era of competitiveness and social progress.**
>
> Jim Hagemann Snabe, Chairman, Siemens

CASE STUDY 1

Moeve's Andalusian Green Hydrogen Valley

Moeve's Andalusian Green Hydrogen Valley – the first phase of which is currently under construction in the industrial area of Huelva, Spain, with a 300-megawatt (MW) electrolyser, the largest in southern Europe – shows how strong regional data ecosystems can accelerate the energy transition through data and technology. By connecting partners across the value chain (such as technology providers, industrial partners and local stakeholders), Moeve's digital-native plants will enable trusted data flows to optimize operations and scale green hydrogen. This model, which forms part of the larger two-gigawatt (GW) Andalusian Green Hydrogen Valley project, underscores the importance of collaboration, common standards and robust governance in Europe.

Source: Moeve.

> **The energy transition demands effectiveness, agility and innovation in equal measure. Decarbonization planning is complex – it requires bringing together energy data, financial parameters and operational constraints across multiple sites and stakeholders to model realistic pathways. The real opportunity is when that capability extends beyond individual companies to entire industrial clusters, where coordinated action on energy, electrification and fuel switching can unlock a scale of impact no single organization can achieve alone.**
>
> Maarten Wetselaar, Chief Executive Officer, Moeve

1 Why data collaboration remains difficult

Structural barriers, including trust gaps, uneven digital maturity, unclear value proposition and systemic cyber risk, limit data collaboration across company boundaries.

Collaboration often stalls when the value proposition is unclear or uneven. In clusters, companies need clarity on funding, ownership and value-sharing to support initiatives.

Despite widespread recognition of the value of data-driven decision-making, many industrial companies still operate with fragmented and underused data. For example, in the European Union (EU), around 80% of industrial data remains unused.[6] This becomes even more pronounced across company boundaries. Insights from the World Economic Forum's Transitioning Industrial Clusters (TIC), Cyber Resilience and Frontier Technologies communities[7] have highlighted four persistent structural barriers that organizations face, limiting their progress in data collaboration.

1 Competitive sensitivity, trust concerns and power asymmetry

Industrial clusters bring together independent organizations with differing regulatory obligations, risk appetites and data sensitivities. Companies are cautious about exposing commercially sensitive information, operational performance data or strategic plans that could weaken competitive positioning or create legal and financial risks. These concerns are often amplified by power asymmetries within the ecosystem, where smaller firms may fear that dominant participants could use shared data to strengthen their negotiating positions or capture a disproportionate share of the value created through collaboration.

Unclear data ownership, security, intellectual property, governance and benefit-sharing mechanisms further limit trust and willingness to share. Without clear rules on control and misuse, organizations tend to restrict data sharing to bilateral exchanges or avoid collaboration altogether.

2 Uneven digital maturity and limited interoperability

Clusters typically include organizations at very different stages of digital development. In 2023, the adoption of Enterprise Resource Planning (ERP) systems in the EU ranged from 37.9% in small enterprises to 86.3% in large enterprises. This shows a significant digital maturity gap among firms, which reflects even broader disparities present in their data infrastructure, system sophistication and technical capability.[8]

Additionally, many organizations continue to operate legacy systems that are not designed for interoperability, while differing data models, standards and formats make consistent data exchange difficult even where technical connectivity exists.

Differences in system upgrade cycles make interoperability all the more complex and unpredictable. If not addressed, these disparities risk complicating collaboration.

3 Unclear value proposition and incentives alignment

Collaboration often stalls when the value proposition is unclear or uneven. In clusters, companies need clarity on funding, ownership and value-sharing to support initiatives. This is especially true where differences in size or capability create concerns about limited returns or competitive risk.

4 Systemic cybersecurity exposure

Cyber risk within clusters is systemic; a vulnerability in one participant can disrupt operations and erode trust across the entire ecosystem. According to Accenture, 72% of organizations report an increase in attacks, and 63% cite the evolving threat landscape as their biggest challenge.[9] In 2024, at least 35.5% of data breaches originated from third-party incidents.[10]

AI amplifies these risks and creates more avenues for malicious actors. A total of 56% of executives believe generative AI gives attackers a clear advantage, while phishing attacks have increased by 1,265% since the launch of OpenAI's ChatGPT.[11]

Cyber resilience in clusters spans multiple stakeholders, shared infrastructure and third-party technologies, often creating uncertainty over accountability. This can weaken trust, as organizations hesitate to connect systems or share data without visibility into others' security posture. When incidents occur, response coordination and learning are often fragmented.

These barriers limit industrial clusters' ability to move towards coordinated system value creation. Overcoming them requires a systemic, phased approach.

2 From shared data to shared value

When organizations share data across boundaries, they unlock outcomes that no single participant could achieve independently.

Data collaboration enables decisions and coordination that no organization can achieve alone by combining information from participants to create ecosystem-level visibility.

It is also a prerequisite for intelligent infrastructure. Industrial clusters need to walk before they can run; effective AI deployment depends on secure, high-quality and well-governed data foundations across organizations.[12] Without them, AI remains confined to isolated optimization and automation rather than unlocking adaptive, semi-autonomous operations that optimize energy, production, logistics, maintenance and resource allocation in real time.

In industrial clusters, many high-value opportunities depend on visibility and cross-organizational collaboration and are grouped into five recurring application areas.

> **Industrial competitiveness is increasingly determined by how efficiently, effectively and securely companies can connect data and infrastructure to optimize the value chain across a wider ecosystem. AI will accelerate productivity, resilience and innovation across the energy and industrial sectors, but the extent of the value generated depends on the scale of collaboration among organizations. The industrial clusters that ensure this collaboration between companies will be best positioned to attract investment, strengthen energy security and lead the next phase of industrial growth.**
>
> Rovshan Najaf, President, State Oil Company of the Republic of Azerbaijan (SOCAR)

FIGURE 1 **Five strategic areas for digital collaboration**

Source: World Economic Forum. (2025). *Five Steps for Digital Collaboration in Industrial Clusters*.

Shared infrastructure development

Large-scale industrial infrastructure often depends on coordination across multiple organizations. Shared visibility into demand, use and operational requirements helps reduce uncertainty, improve resource allocation, optimize the business case and support investment decisions that individual participants could not optimize independently.

> **The energy transition is not only about changing the energy we use. It is also about changing how industries work together. Shared infrastructure, better coordination through data and new technologies will be critical to building more integrated and competitive industrial ecosystems with lower emissions.**
>
> Josu Jon Imaz, Chief Executive Officer, Repsol

CASE STUDY 2

H2Integra in the Net-Zero Basque Industrial Super Cluster | coordinating shared hydrogen infrastructure through data collaboration

H2Integra, led by Petronor (Repsol) and supported by a consortium of 12 co-located organizations across the Net-Zero Basque Industrial Super Cluster, is building an integrated green hydrogen value chain linking a 2.5 MW electrolyser in Muskiz with industrial off-takers, refuelling stations, port operations and a data centre.

The project addresses one of the core challenges of shared industrial infrastructure: investment decisions across the value chain are highly interdependent. Electrolyser operators, infrastructure providers, logistics operators and industrial consumers all depend on confidence that sufficient demand and operational coordination exist across the ecosystem. Pooling projected demand from steel, aluminium packaging, mobility and backup power systems gave participants a clear view of aggregate future consumption, with enough certainty to support infrastructure investment decisions.

But coordination doesn't end there. Once operational, the system will use a shared digital coordination layer to balance hydrogen production, compression, storage, logistics and distribution across the cluster. Participants will contribute real-time demand information to a platform developed by IBIL and enabled by the internet of things (IoT), supporting operational coordination without exposing sensitive data to other participants, while Petronor will use AI-driven forecasting models to optimize generation on an hourly basis.

The project demonstrates how data collaboration can help industrial clusters coordinate investment planning, improve infrastructure use and operate shared assets as a connected ecosystem rather than as isolated facilities.

Source: The Net-Zero Basque Industrial Super Cluster.

Operations and process optimization

Shared operational visibility and coordinated action allow organizations to optimize scheduling, logistics, maintenance and resource allocation across the ecosystem.

CASE STUDY 3

Qingdao Port automated terminal | cross-stakeholder data sharing as the basis for full-domain operational coordination

Container ports face structural complexity that traditional segmented operations cannot resolve. Vessels have grown in size, schedules have tightened and cross-border supply chains demand greater timeliness and stability – yet operational coordination across berths, quay cranes, yards and inland distribution has historically relied on isolated systems and experience-based scheduling. At Qingdao Port's automated terminal, one of the world's largest automated container hubs, isolated information between port operators, customs authorities, shipping lines, truck fleets, freight forwarders, port inspection units and cargo owners limited both end-to-end visibility and the terminal's ability to dynamically allocate resources.

To address this, Qingdao Port has deployed a full-domain intelligent operations system anchored in two integrated platforms: the Automated Terminal Intelligent Control System (A-TOS), which serves as the central decision-making layer, and the Automated Equipment Control System (A-ECS), which executes scheduling instructions across the terminal's physical assets. Together, they converted disconnected processes – segmented by function and by organization – into a single data-driven workflow that spans both the terminal's internal operations and its external stakeholders.

From an operational perspective, the system supports a more targeted and secure exchange of data among supply chain actors. Shared data covers vessel berthing schedules, container handling instructions, yard slot status, equipment conditions, customs filings, truck appointments and end-to-end logistics milestones – interacting in milliseconds to keep scheduling decisions synchronized with on-site execution. Data sharing follows a hybrid model combining standardized open application programming interfaces (APIs), interconnection with public port data platforms, dedicated secure lines and on-demand targeted pushing, balancing collaborative efficiency with regulatory and security requirements. The data platform itself is operated and governed by Qingdao Port, with access controls, audit trails and supervisory mechanisms aligned with national port data and privacy regulations.

The scale of the operational gains illustrates the impact of this approach. Since deployment, the terminal has recorded a 6% increase in overall service efficiency, a 26% improvement in yard storage capacity and a 14.2% increase in handling efficiency, with peak single-machine productivity reaching 67.76 twenty-foot equivalent units (TEUs) per hour. Truck turnaround time within the port has been cut by more than half.

Source: Qingdao Port.

Resource efficiency and circularity

Industrial clusters often contain significant opportunities to reuse waste, by-products, excess heat and unused materials across organizations. Shared visibility into resource flows helps participants identify and coordinate circularity opportunities across the ecosystem.

CASE STUDY 4

Kalundborg Symbiosis | making resource flows visible to enable industrial symbiosis at scale

Industrial sites typically optimize their own resource flows in isolation, treating water, heat and material by-products as waste rather than potential inputs for neighbouring operations. The information needed to identify cross-company reuse opportunities exists within individual facilities, but without shared visibility across organizational boundaries, they remain invisible.

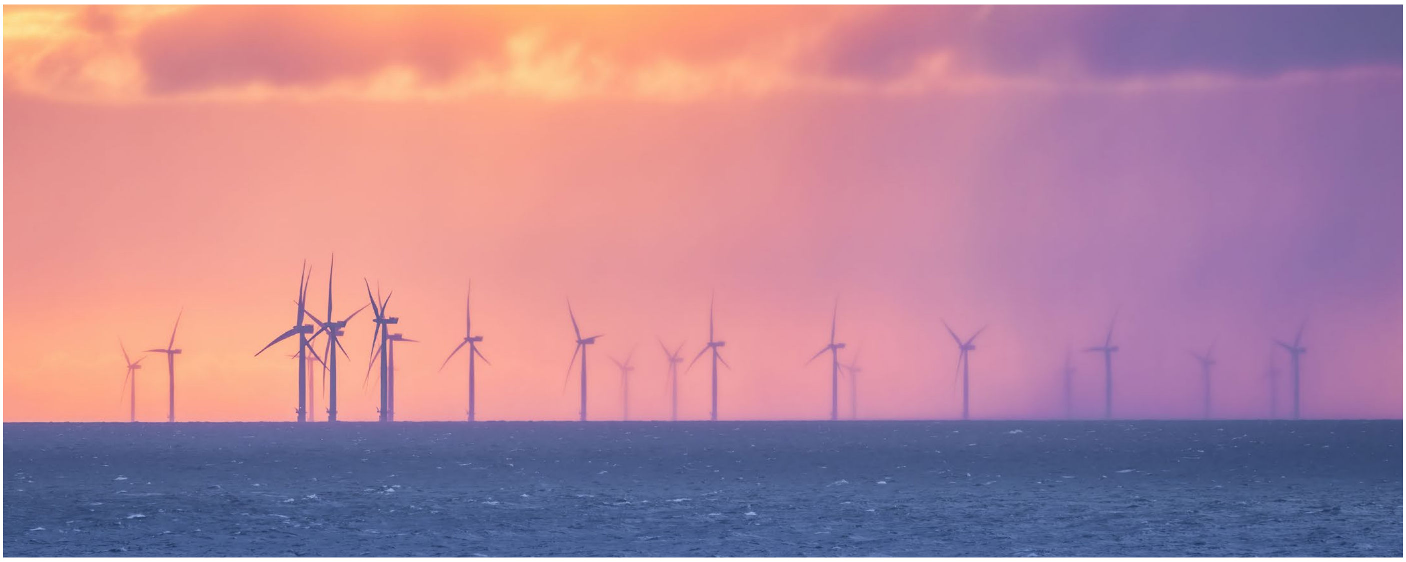
Kalundborg Symbiosis in Denmark has addressed this challenge over five decades, building the world's first industrial symbiosis into a partnership of 17 public and private organizations spanning pharmaceuticals, biosolutions, energy, utilities, logistics and municipal entities. The defining principle is straightforward: a residual flow from one organization becomes a resource input for another. Surplus heat from one site becomes process energy for a neighbour; treated water from one facility replaces groundwater at another; biotechnology by-products are valorized as feedstock rather than disposed of as waste. Across the cluster, more than 35 streams of water, energy, materials and residual outputs are exchanged.

A central database, managed by the secretariat, documents member companies and resource flows and supports the visualization, coordination and identification of new symbiosis opportunities. This shared information transforms fragmented bilateral awareness into a coherent map of the cluster's resource flows. The data layer currently relies on human operators to interpret and act on those connections; meanwhile, the secretariat is exploring how AI-driven matchmaking could automate and accelerate the identification of opportunities.

The AI-driven tools will also support investment decisions on new infrastructure and help prioritize circular resource use. Kalundborg Utility is collaborating with European partners to develop models that map and distribute all existing and future water sources – both new and reused. These models help determine the infrastructure required for basic utilities and design systems that prioritize resources in line with the circular cascade use identified in the symbiosis database.

The outcomes at Kalundborg demonstrate what shared resource visibility can unlock at the cluster scale. The symbiosis conserves approximately 4 million cubic metres of groundwater each year (a growing volume), recycles more than 200,000 tonnes of residual materials and has reduced overall emissions within the cluster by approximately 80% since 2015. This positions the wider Kalundborg industry to better meet demand in a world of increasing pressure on natural resources.

Source: Kalundborg Symbiosis.



Commercial optimization and trading

Industrial clusters largely engage with external markets – for energy, commodities, capacity and services – as individual companies, often limiting their ability to fully capture the value of shared assets and market opportunities. By coordinating commercially across co-located organizations, clusters can optimize asset use, aggregate demand, pool flexibility and participate in markets at scale. The result is more competitive contracting, better risk management and new revenue streams from the ability to significantly expand market capacity as well as new services such as grid flexibility and demand response.

CASE STUDY 5

Port of Esbjerg | using a digital twin to unlock commercial growth in offshore wind

As offshore wind scales rapidly across the North Sea – targeting up to 65 GW by 2030 and 150 GW by 2050 – ports have become critical commercial infrastructure within the value chain, enabling the shipment of installation components and the handling of increasingly complex logistics flows. For the Port of Esbjerg, this represented a significant market opportunity, but one that traditional planning approaches, based on static assumptions and fragmented data, were insufficient to capture.

To address this, the Port of Esbjerg developed a digital twin, a virtual replica of its infrastructure and operations, integrating data from port assets, logistics flows and operational processes into a unified simulation environment. The digital twin aggregates large datasets – including infrastructure characteristics, historical operations and process data – and applies simulation and machine learning (ML) techniques to model different scenarios. This allows the port to test capacity configurations, evaluate trade-offs and optimize the use of port land and infrastructure under demand conditions.

The commercial impact is significant. By improving forecast accuracy and enabling dynamic capacity allocation, the port can make more reliable and competitive commitments to offshore wind developers, turning operational visibility into a commercial advantage.

The digital twin is expected to support handling of approximately 4.5 GW of offshore wind components – around three times its previous level – directly expanding the port's revenue potential in a fast-growing market.

The port is currently exploring the opportunity to extend the digital twin to connect data across the broader offshore wind supply chain – from component production to installation – or across multiple ports, enabling coordinated market participation at the ecosystem level.

Source: Port of Esbjerg.

> **The next phase of competitiveness will not be won through infrastructure alone. It will depend on how effectively industrial clusters combine shared infrastructure, digital innovation and trusted data collaboration to drive efficiency, decarbonization and lasting value.**
>
> Dennis Jul Pedersen, Chief Executive Officer, Port Esbjerg

Environment and risk management

Environmental and operational risks in industrial clusters frequently extend across multiple organizations. Shared situational awareness improves monitoring, preparedness, compliance and coordinated response capabilities across the ecosystem.

> **Environmental and operational risks do not stop at a single company's fence line. Shared situational awareness and coordinated response transform fragmented, company-by-company exposure into a collective resilience capability for the entire cluster.**
>
> Rogério Zampronha, Chief Executive Officer, Prumo Logística

CASE STUDY 6

Port of Açu | shared operational intelligence for coordinated risk management

The Port of Açu, the largest private port-industrial cluster in Latin America, hosts approximately 30 companies and 11 terminals across the oil and gas, mining, logistics and industrial sectors. Its ecosystem includes global companies such as Baker Hughes, Equinor, TotalEnergies, Shell and Repsol.

Managing operational and environmental risks within such a concentrated industrial cluster requires continuous, real-time visibility over weather conditions, maritime traffic, navigational safety and emergency response activities. Recognizing that individual companies were often collecting and managing similar information independently, the port developed a centralized operational coordination capability through its Center of Operations and Response to Emergencies (CORE).

CORE integrates metocean, maritime, operational and security data into a shared situational awareness platform. The system combines vessel traffic services (VTS), emergency coordination, security monitoring and hyperlocal metocean forecasting into a unified operational framework.

Rather than implementing a fully standardized collaboration platform from the outset, the Port of Açu adopted a pragmatic, incremental approach. Operational information is currently shared with tenants and industrial users according to their specific operational requirements. Over time, this model is expected to evolve into a more structured data-as-a-service capability, enabling broader data integration and collaboration across the cluster.

The shared monitoring and coordination capability enhances navigational safety, supports weather-sensitive operational planning, strengthens pollution-prevention efforts and enables more effective emergency-response coordination. It also reduces duplication of monitoring infrastructure and resources among participating companies.

This case demonstrates how shared operational intelligence can enhance resilience, improve environmental risk management and create collective value across complex industrial ecosystems.

Source: Port of Açu.

3 Turning strategic ambition into action

Closing the gap requires sequencing the right moves in the correct order.

For industrial clusters to realize their full value, they must coordinate across organizations with different incentives, capabilities, priorities, risk appetites and ways of working.

Successful data collaboration, therefore, requires not only technical enablement, but also behavioural alignment between participants, clear governance, trusted partnerships and effective decision-making structures.

To help industrial clusters move from strategic ambition to execution, this chapter outlines a practical three-stage approach to extract value from data collaboration.

FIGURE 2 **Three stages of data collaboration**

Iterate

Stage 1: Value case

Translates strategic opportunity into concrete use case

- **Value opportunity identification** (Where system value can be unlocked)
- **Use case definition** (Action, decision, or outcome enabled through data collaboration)
- **Business case calculation** (Expected benefits vs investment requirements, operating costs and risks)

Stage 2: Enablement

Defines the **collaboration model** and sets up data collaboration mechanisms through:

- **Data governance**
- **Data readiness**
- **Technology**

And **cyber resilience** as a cross cutting layer

Stage 3: Execution

Turns data collaboration into measurable outcomes

- **Use case value tracking and monitoring** (KPIs, ROI, impact measurement)
- **Scaling** (Identification of new features, participants, and use cases)
- **Unlocking innovation** (New services, optimization opportunities and business models)

Stage 1: Defining the value case

In the value case stage, clusters define concrete digital collaboration use cases that support their strategic objectives and contribute to the creation of system value[13] outcomes.

System value covers not only financial but also social, environmental and compliance outcomes, helping stakeholders prioritize actions that accelerate business progress while creating broader benefits.

Prioritized use cases must be underpinned by a clear business rationale, including expected benefits, investment requirements, operating costs, risks and how these are allocated across participating organizations as well as an understanding of the relevant data requirements.

The case for data collaboration becomes self-evident to participants when they understand what digital applications can deliver at the cluster level.

Central to this work is the orchestrator role. Rather than controlling data or making decisions for participants, the orchestrator provides institutional trust and turns shared visibility into coordinated action across participating organizations. Many opportunities stall despite a strong business case because organizations are not aligned on timing, ownership or execution. A neutral convenor or trusted institution can close this gap by mobilizing stakeholders, aligning sequencing and maintaining momentum across organizational boundaries.

To sustain this momentum, clusters should adopt a phased approach that unlocks value over time, balancing near-term results with strategic initiatives in a portfolio roadmap. Without a clear value proposition, support for leaders or tracking mechanisms, collaboration often loses commitment.

The objective is to create a robust and modular foundation that supports initial use cases while being designed for expansion in line with portfolio needs.

Stage 2:
Designing and implementing the data collaboration model

In the enablement stage, the data collaboration model is designed in detail and implemented.

This includes defining the data architecture, interoperability standards and governance mechanisms required to support secure and trusted collaboration. Key design choices include how data is managed throughout its life cycle and how responsibilities and decision rights are allocated among participants.

The objective is to create a robust and modular foundation that supports initial use cases while being designed for expansion in line with portfolio needs. Four pillars make this possible: data governance defines how data is managed and used; data readiness ensures it can be understood, trusted and reused across organizations; technology provides the infrastructure to share and access it effectively; and cyber resilience underpins all three, embedding trust, security and operational continuity into every interaction.

Stage 3:
Executing and scaling applications

In the execution stage, the projects become operational and start delivering value. The focus shifts to operating and scaling them – monitoring performance, tracking value realization and identifying new features, participants or applications that can be added at lower marginal cost. As a shared data foundation is established, additional organizations, datasets and use cases can be integrated more easily. Following an iterative approach, new use cases are built on existing capabilities, informing the evolution of the implementation roadmap and unlocking new value opportunities. This creates incentives for broader participation and sustained engagement over time.

Data collaboration can also support innovation across the ecosystem. Fragmented data across companies and technologies limits visibility, coordination and innovation in complex networks.[14] Shared data can shift innovation from isolated pilots to sustained, ecosystem-wide experimentation, driving long-term value creation.

“Our role goes beyond being a landlord – we are responsible for ensuring that companies in our cluster have access to clean, affordable energy. Our digital project Starlings in Botlek shows how this works in practice: we act as an orchestrator and bring the right partners together, start with a clear use case and deliver tangible value early. Trust builds, and with it, the conditions for innovation at scale.

Boudewijn Siemons, Chief Executive Officer, Port of Rotterdam

CASE STUDY 7

Starlings at the Port of Rotterdam | unlocking industrial flexibility through a value-first, iterative approach

The Starlings Project at the Port of Rotterdam shows how a value-first, iterative approach can work in practice, as well as the key role of the orchestrator.

The Port of Rotterdam, located in the Netherlands, is the largest seaport in Europe and a major logistics hub. It also hosts one of Europe's biggest industrial clusters, which incorporates companies from oil and gas, petrochemicals, chemicals, logistics and heavy industry.

To respond to rising energy costs and improve resilience, the cluster launched the Starlings Project in 2025, aiming to help companies trade utilities such as electricity, steam and hydrogen in real time.

The project was led by the Port Authority, which acted as the orchestrator. The Port Authority started with a clear business case and brought together the right partners early on – industrial players, technology providers and grid operators. To build trust and momentum, it invested €2 million and set up a three-phase pilot focused on delivering short-term results.

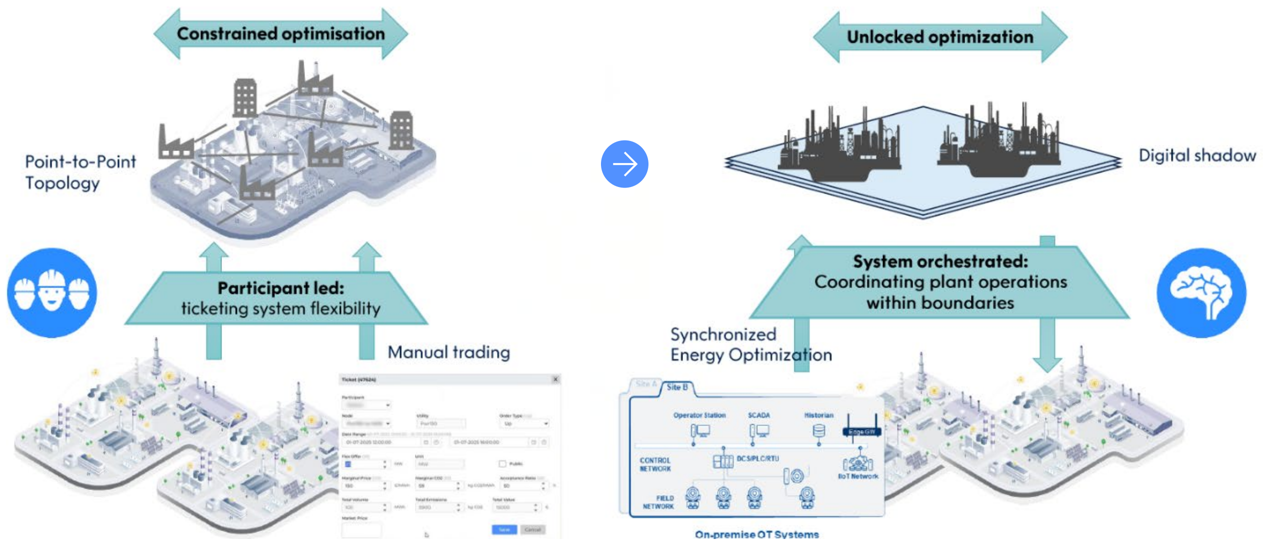
At the project's core is an energy management system that allows companies to adjust utility flows across the cluster in near real time – for example, turning rigid contracts into flexible, value-creating interactions. Imagine two sites with a physical connection and a contract to exchange steam. One site may want to reduce its use, while the other can lower supply if compensated. The platform matches these needs: if the value of reducing demand is higher than the cost of reducing supply, a deal is made. In practice, this means lower costs, lower emissions and better use of existing infrastructure.

Instead of building a full digital solution from day one, Starlings started with a simulation and a simple, modular design focused on the initial use case, with the option to expand over time. The platform was built to ensure security and confidentiality; only flexibility bids ("tickets") were shared, not sensitive operational data.

The pilot ran in three phases, each building on the last. The first two trials showed strong participation and helped build trust across companies. They also delivered tangible results, including efficiency gains of around 5%, and helped put energy management back on the agenda at the cluster level.

The third trial went further. It explored deeper data collaboration and looked beyond optimizing existing assets. This included moving away from manual to automatic system-level optimization and introducing the idea of jointly investing in shared infrastructure, such as a high-efficiency combined heat and power (CHP) plant or more buffers, to share risks (such as redundancy) across cluster members. With more advanced data sharing, better system-wide optimization and improved platform capabilities, benefits could more than triple compared to earlier trials. Adding shared infrastructure could increase them even further, up to 8.5 times the original value.

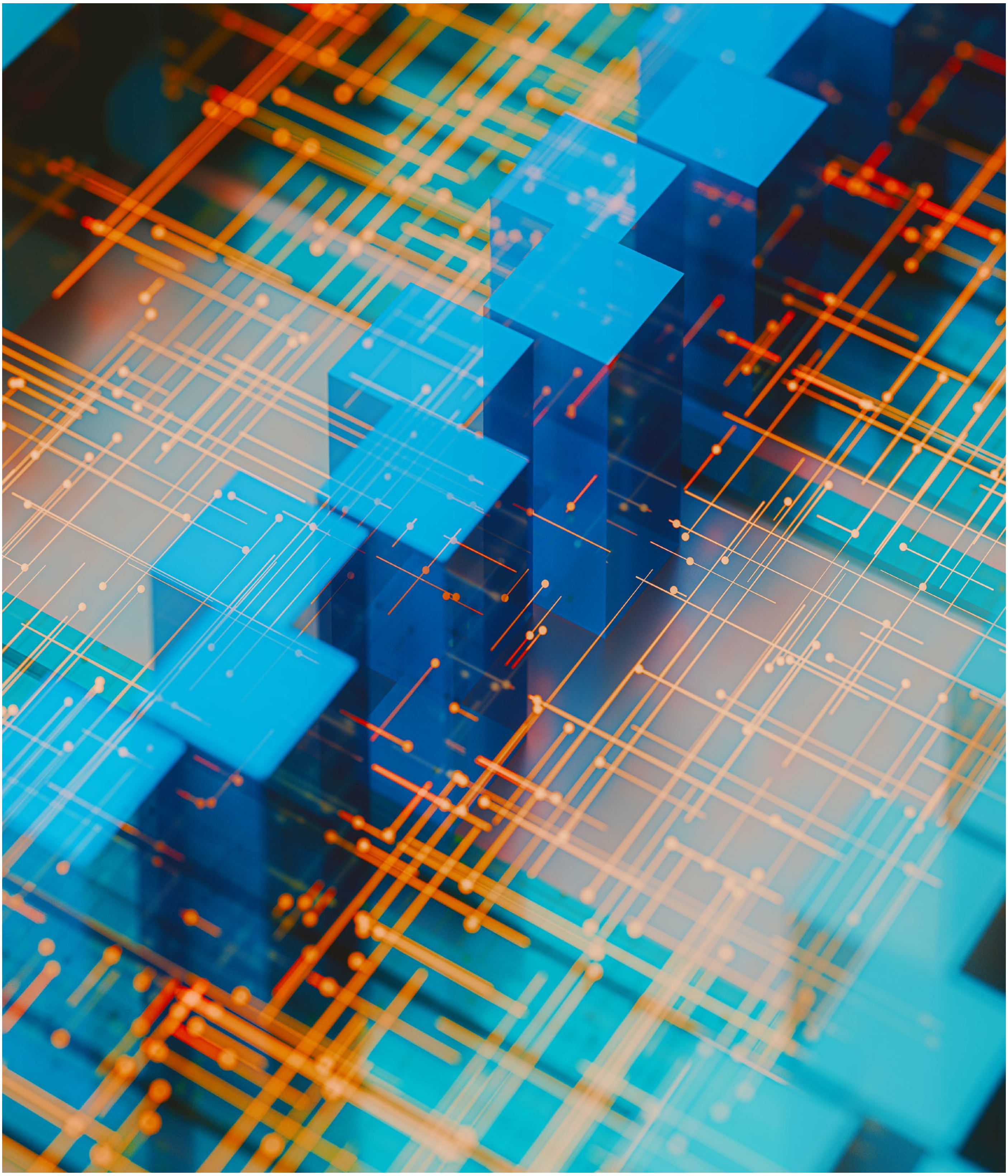
This shows that real value doesn't just come from trading flexibility, but from shaping a multi-commodity energy system and investing together where it makes sense. The next phase will focus on exchanging more granular, real-time data from operational assets, improving system integration and developing investment-ready plans for shared infrastructure. All of this will be collaborative, without requiring upfront funding from participants.



Source: Port of Rotterdam.

4 Building the enabling foundations

Scalable data collaboration depends on foundations that are built in from the start.



This chapter elaborates on the four pillars introduced in Stage 2 – data governance, data readiness, technology and cyber resilience – the interdependent foundations that clusters must design and implement to move from strategic ambition to operational execution.

Data governance defines how data is managed, controlled, accessed and used. **Data readiness** ensures shared data can be interoperable, understood, trusted and reused across organizations. **Technology** provides the infrastructure and tools to share, access and use data effectively. **Cyber resilience** protects the integrity and security of the system.

The design choices across these four dimensions are not independent: they interact and reinforce one another, and must be calibrated to the collaboration model the cluster adopts.

FIGURE 3 **Data collaboration framework**

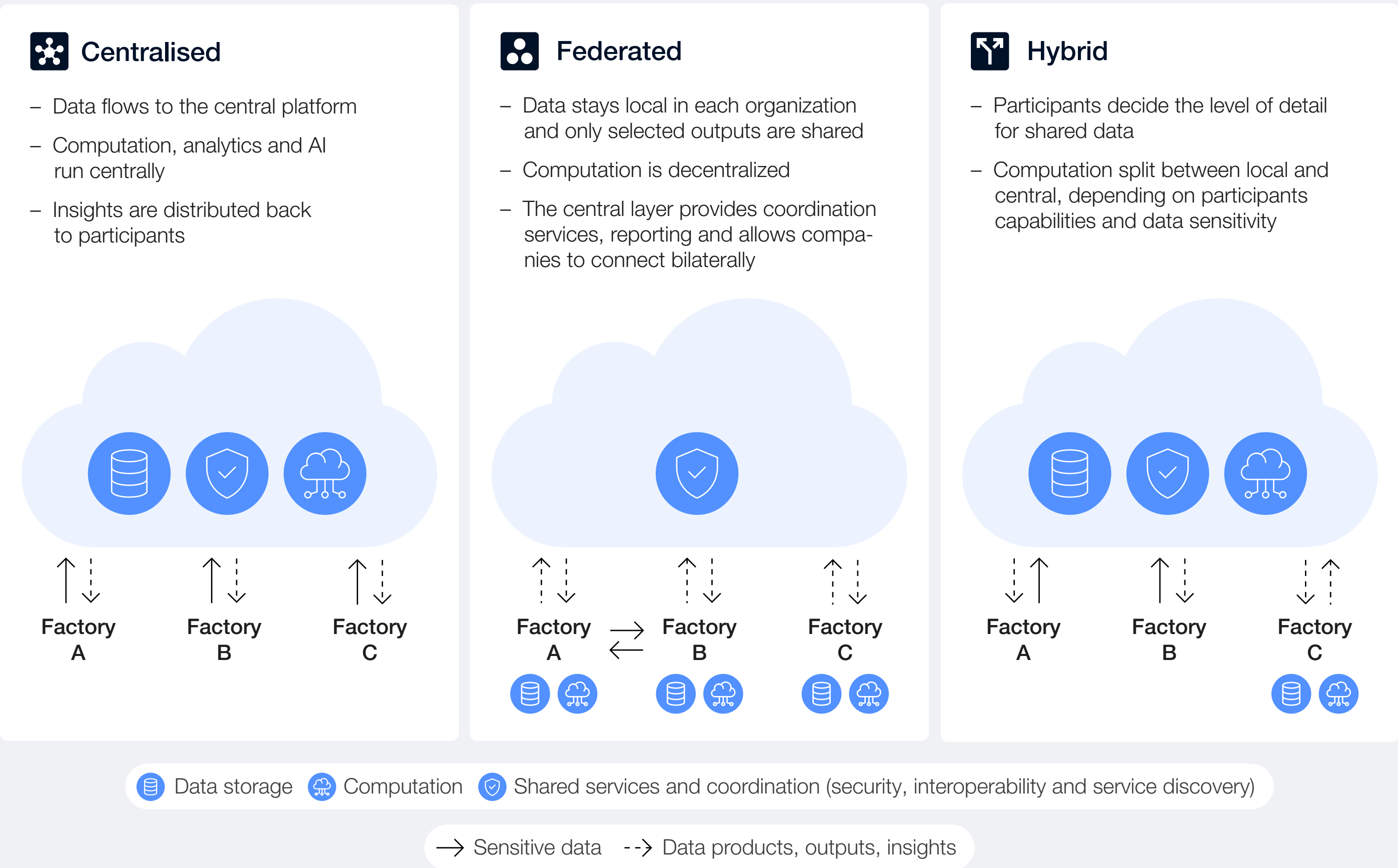
4.1 Collaboration models

A spectrum of data collaboration

Data exchange in industrial clusters can take different forms in practice, and the collaboration model adopted shapes the governance, technology and security requirements that follow. Models exist on a spectrum from centralized to federated setups, determined by three key design choices:

- **Where data resides and how much of it moves across organizational boundaries**: whether data is consolidated in a shared hub or remains within participant systems, with only selected outputs or data products shared
- **Where computation happens**: whether analytics, optimization and AI models run centrally on pooled data or locally, with only approved aggregated results exchanged
- **What role the central hub plays**: whether it acts as a full data platform for data storage, exchange and processing, or merely as a marketplace or coordination layer that enables orchestration and bilateral exchange

FIGURE 4 **Data collaboration models**



Hybrid models have emerged as the most common approach across leading industrial ecosystems – reflecting the reality that effective cluster collaboration requires both local control and shared coordination.

Centralized model

In a centralized setup, selected data from participating organizations is copied or streamed to a central platform. The platform stores and processes the data, making it available for approved use cases across the cluster. The central platform becomes the primary data environment, running analytics, optimization and AI models on pooled data, and distributing insights and coordination instructions back to participants. Each organization's own systems primarily act as data sources.

Data can be sanitized before sharing through aggregation, masking, anonymization or synthetic data generation, and access controls further limit who can use what, but the defining feature of this model is that data flows to the central platform. This makes it technically accessible to the platform operator and therefore this collaboration model requires a high degree of trust and robust governance to be acceptable.[15]

Centralized models enable the most powerful shared analytics and the tightest coordination, but they require participants to hand over a degree of control over their data.

Federated model

In a federated data collaboration setup, data remains within each participant's own systems and is not pooled into a central environment. Computation happens locally, with participants running analytics and transformations on their own data. Outputs that carry little sensitivity risk – including aggregated metrics such as key performance indicators (KPIs) and signals, or derived insights such as forecasts and optimization results – cross organizational boundaries.

A practical example is federated learning, where AI models are trained locally on each participant's data, and only the resulting model weights – not the underlying data – are shared and aggregated into a common model. This allows the cluster to benefit from collective intelligence without any participant exposing their raw data.[16]

The central coordination layer serves three lighter functions. For reporting, it aggregates and displays cluster-level outputs, such as shared KPIs, emissions dashboards and performance metrics, using transformed data contributed by participants. For coordination and discovery, it enables organizations to discover available services, publish their own capabilities – such as excess heat, storage capacity or flexibility – and connect with relevant counterparties. As an interaction and security layer, it provides the technical infrastructure that enables federated exchange and ensures its trustworthiness. Storage and processing in the central layer are limited to what is required for reporting and coordination.

This model is particularly suited to contexts where competitive sensitivity or regulatory constraints render any transfer of granular data unacceptable.

Hybrid model

In practice, most industrial clusters adopt a hybrid approach, combining elements of both models. Sensitive or operational data remains within each organization's systems and is processed locally; selected datasets or derived outputs are shared with a central platform to support cross-company analytics, reporting and coordination. Participants can choose the level of detail to contribute, allowing the model to adapt to their comfort level with sharing data.

Hybrid models offer three advantages: they balance data sovereignty with coordination capability – organizations still choose what to share and at what level of detail, keeping sensitive data local if needed, while shared outputs enable cluster-level insights. They accommodate differences in digital maturity and willingness to share, allowing organizations to participate at different levels without being excluded. They also support gradual onboarding, enabling clusters to start with limited sharing and deepen their collaboration as trust develops.

As a result, hybrid models have emerged as the most common approach across leading industrial ecosystems – reflecting the reality that effective cluster collaboration requires both local control and shared coordination.

CASE STUDY 8

Factory+ | centralized and hybrid data collaboration models in practice

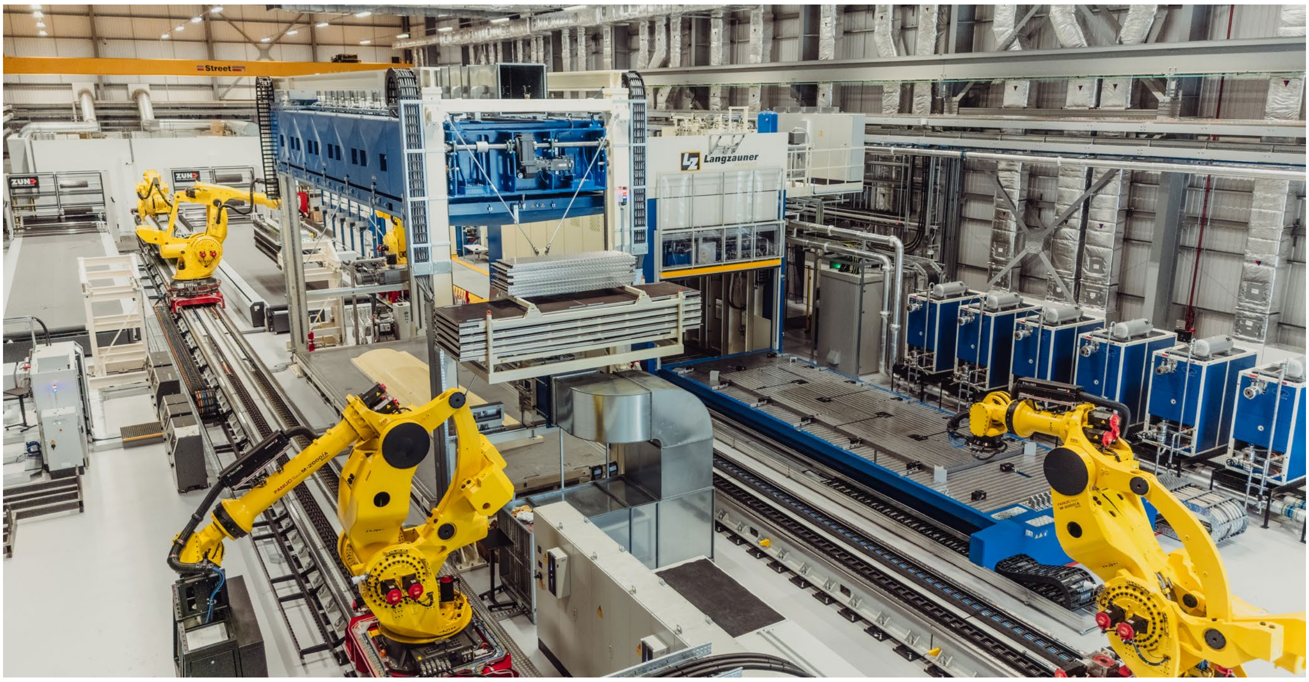
The Factory+ platform, developed by the University of Sheffield's Advanced Manufacturing Research Centre (AMRC), shows how data collaboration can be implemented across industrial environments. Designed as a modular IoT infrastructure, Factory+ connects industrial assets via a combination of central and edge components, enabling data collection, standardization, and exchange across manufacturing systems.

Factory+ allows the same architecture to be deployed in different configurations, ranging from centralized to hybrid setups, depending on the requirements of the participating organizations.

In a **centralized** deployment, Factory+ operates as a single centralized IoT infrastructure. The central platform hosts a time-series database for storing telemetry data – real-time measurements and operational signals transmitted continuously from connected machines and sensors – a configuration database that manages the status and configuration of connected components and a repository of frameworks that define how data is structured. It also includes a message queueing telemetry transport (MQTT) broker for data from edge devices, making it available to data consumers, as well as services for visualization and basic analytics. Access control and system configuration are managed centrally. Edge platforms are positioned nearer to the machines and oversee edge agents that gather and organize data from industrial equipment prior to sending it to the central broker. Centrally defined frameworks enforce data standardization, and configuration is distributed from the central cluster to the edge in a controlled, top-down manner. In this setup, data from across the environment is collected into a single shared infrastructure, where it can be accessed and used within the same system.

Factory+ also supports a **hybrid** configuration, in which each organization operates its own platform instance, retaining control over local data storage, authentication, and edge configuration. Using MQTT bridging, organizations can share selected telemetry data while controlling it, limiting or revoking access when required. This enables them to feed data selectively into a shared data store while still retaining a local database for all their data. The data shared with other organizations could be an aggregate of the raw telemetry data that they collect, or the results of analytics performed on their telemetry data. To ensure that the quality and structure of telemetry data are consistent across organizations, the separate instances can pull schemas from a shared repository. This repository is live, so if one organization creates a schema that doesn't yet exist to meet its requirements, it can share it with other members of the cluster to avoid the effort of reproducing it.

A practical example is the AMRC's open-access Composites at Speed and Scale (COMPASS) facility, which has Boeing as its first user. A dedicated Factory+ instance is deployed for COMPASS activities, with data stored separately from other AMRC telemetry. At the same time, selected data values are shared with the wider AMRC environment via an MQTT bridge, enabling reuse across IoT and data science applications. The COMPASS instance retains full control over the data shared, while interoperability is maintained through shared schema repositories, ensuring consistent interpretation across systems.



Source: Advanced Manufacturing Research Centre (AMRC).

CASE STUDY 9

Kopernikus SynErgie | enabling cluster-level energy flexibility through a federated data collaboration model

The SynErgie project, led by the University of Stuttgart and Fraunhofer, demonstrates how a federated data collaboration model can support cluster-level energy flexibility while preserving data sovereignty.

Industrial clusters can help stabilize power systems by coordinating energy consumption, generation and storage across co-located assets. However, this potential is often limited by fragmented data landscapes, heterogeneous systems and concerns about sharing commercially sensitive operational data.

SynErgie addresses this challenge through a federated architecture that lets companies optimize energy use and provide flexibility services to the grid without centralizing operational data.

In the federated setup, data remains within individual company platforms operated by each participating organization. A separate central market platform (CMP) acts only as a coordination and marketplace layer. It does not store or process operational data, but enables companies and service providers to publish, discover and connect flexibility services such as peak-shaving optimization, price forecasting or flexibility aggregation. Data exchange occurs directly between participants rather than through the CMP.

To enable interoperability across different company platforms and with the CMP, Fraunhofer developed the Energy Synchronization Platform (ESP) – a blueprint for configuring company platforms. It is available as open source, along with a reference implementation to support adoption.

In addition, Fraunhofer developed the Energy Flexibility Data Model (EFDM), which standardizes how energy flexibility is described and exchanged between company platforms and service providers through open-source specifications and JavaScript Object Notation (JSON) schemas. While data requirements vary by service (e.g. industrial demand response, ancillary service markets, etc.), the EFDM's design principle – as few mandatory attributes as possible – ensures that companies can participate across different contexts without over-exposing sensitive data.

Participating organizations can manage access control via their company platforms. Each company defines what data is shared, with whom and under which conditions. While common mechanisms such as public key infrastructure (PKI) and role-based access control provide a technical foundation, enforcement remains decentralized.

This approach has been implemented in the FlexQuartier use case in Augsburg, Germany. In this small industrial cluster, Alois Müller and several smaller firms operate in close proximity, each using its own company platform. Alois Müller plays a central coordinating role, acting as an aggregator of flexibility. This role is enabled by its ownership of the largest heat buffer storage in the cluster and by its position as the project's initiator, which naturally made it an anchor for cross-company coordination.

SynErgie demonstrates that effective data collaboration in industrial clusters does not require centralizing data. Instead, value is unlocked by combining local data control with shared coordination services and standardized interfaces, enabling scalable and secure collaboration across independent organizations.

Source: Fraunhofer.

4.2 Data governance

Enterprise data governance versus cluster data governance

Data governance defines how data is managed, controlled, accessed and used. It requires establishing decision rights, accountability structures, policies, standards and control mechanisms.

However, when **data moves beyond organizational boundaries, data governance becomes significantly more complex**. Data collaboration in clusters requires competitors, suppliers and operators to exchange information under shared rules. In this context, governance is no longer just about internal control; it becomes the institutional mechanism that enables trust, interoperability, fair value allocation and regulatory compliance.

Cluster data governance framework

To function at scale, data collaboration in industrial clusters requires a data governance framework – **a set of interdependent components that define how collaboration operates in practice.**

FIGURE 5 | **Cluster data governance framework**

1 Institutional governance	Who decides?
2 Economic and incentive models	Why participate?
3 Legal and contractual frameworks	What is allowed?
4 Policies, standards and procedures	How is data used?
5 Trust and compliance mechanisms	How is trust enforced?

1 **Institutional governance** establishes formal governance bodies, their composition and their decision rights. It also defines how conflicts between participants are resolved and how new participants are onboarded.

2 **Economic and incentive models** define how investment costs are allocated, how benefits are measured and distributed and how contributions (e.g. data provision, investment, participation) are recognized and incentivized.

3 **Legal and contractual frameworks** provide the enforceable foundation for collaboration between parties with different legal obligations, risk profiles and competitive positions. At the core are multilateral data-sharing agreements that set the rules of engagement for participants, dispute-resolution mechanisms and exit provisions. Beyond contractual safeguards, data sovereignty requirements directly influence the design of the data-sharing architecture. Decisions on where data is stored, processed, and accessed must align with jurisdictions and sector-specific regulations. In practice, this often limits cross-border data movement and reinforces the need for federated or hybrid architectures, where sensitive data remains within defined legal boundaries.

4 **Policies, standards and procedures** translate legal principles and governance decisions into operational rules that can be implemented consistently across organizations and systems (Figure 6).

5 **Trust and compliance mechanisms** ensure that governance rules are applied and enforced. Ensuring compliance requires tracking adoption of mandated activities, setting up and monitoring KPIs. These mechanisms can be supported by organizational processes and technical controls (e.g. logging, identity management, monitoring systems), providing transparency and accountability across the ecosystem.

FIGURE 6 | **Policies, standards and procedures**

Data policies
Norms and rules of operation

Definition and formats

Policies for data definition and formats to ensure consistent business meaning across systems and participants

Classification

Categories: open, shared, restricted and confidential

Access

Data is used only by authorized parties and for permitted purposes only

Retention

Governing how long data is maintained and when it is disposed of

Data standards
Criteria and specifications

Naming conventions

Data naming conventions and attributed formatting standards for the definition, creation, storage and use of data

Quality metrics

Data quality metrics and backup requirements

Classification metadata

Standardized representation of classification and access attributes in metadata, ensuring consistent interpretation and enforcement across systems

Data procedures
Execution of governance processes

Managing definitions

Managing and publishing data definitions; assigning/maintaining data classification

Enforcing rules

Enforcing access and use rules and supporting operational processes (e.g. analytics, predictive modelling)

Data products

Defining how data is exposed as reusable data products within the ecosystem, ensuring data shared by different participants can be used safely and consistently

Cluster data governance organizational structure

While cluster-level data governance operating models vary across contexts, the following four institutional bodies – each with distinct and complementary roles – typically feature in mature cluster governance models. The **governance board** sets strategy and resolves disputes; the **governance office** translates decisions into operational rules; **data owners** retain control over their data; and the **neutral orchestrator** convenes stakeholders from across organizational boundaries.

FIGURE 7 **Cluster data governance operating model**

Cluster data governance board
Strategic authority

Senior representatives from participating companies and legal/regulatory expertise

- Sets institutional governance, defines economic models and incentives, allocates budget
- Approves data initiatives and governance frameworks (contracts, policies, standards)
- Resolves disputes between participants

Cluster data governance office
Working body

Data architects and experts in security, legal, data governance

- Develops shared data models, interoperability standards and access control frameworks
- Produces implementation guidelines; in mature clusters, may be a dedicated central expert team
- Translates board decisions into operational rules consistently applicable across organizations

Data owners
Each participating organization across the cluster

- Accountable for the value, risk and lawful use of their data (holds decision authority over whether data is shared, for what purpose and under what conditions)
- Define use rights and approve participation in data products and use cases
- Ensure compliance with legal, regulatory and commercial constraints
- Responsible for data quality
- Ownership always originates and remains with the contributing organization, even when shared or processed externally

Separate enabling role

Neutral orchestrator
Typically a cluster convenor or neutral trusted organization, such as a port authority

Early stages
Convenes stakeholders, shapes the initial collaboration agenda and supports establishment of governance structures

As governance matures
Becomes embedded within governance structures, shifting towards ongoing coordination and execution support

Advanced stages
Acts as a coordination engine, sustaining collaboration, resolving stalls and maintaining momentum across the ecosystem

Increasingly, AI and advanced data technologies can help operationalize governance and strengthen trust across industrial ecosystems.

New derived data products can be created in models that combine and transform data at the cluster level. In such cases, ownership does not transfer in the traditional sense but is instead extended to a shared or governed model.

This means that:

– Contributing data owners retain rights over how their data is used and can impose restrictions or revoke access.

– Companies can use agreed-upon use rights to govern cluster-level data products.

– A designated accountable party (e.g. cluster operator or governing body) may act as the operational "owner" of the data product, responsible for its management, access control and compliance enforcement.

AI as data collaboration enabler

Increasingly, AI and advanced data technologies can help operationalize governance and strengthen trust across industrial ecosystems. AI-enabled tools can support automated data classification by identifying sensitive or business-critical information, validate datasets against agreed requirements for format, completeness, metadata and permitted use, and streamline governance processes through workflow triage and automation of approvals, access requests and exception handling. In parallel, privacy-enhancing technologies allow organizations to analyse and derive insights from shared data while limiting exposure of the underlying inputs. These capabilities are particularly valuable in industrial clusters, where governance processes must operate across organizations, systems and varying levels of digital maturity.

TABLE 1 **Summary of data governance across collaboration models**

Centralized	Federated	Hybrid
– Requires strong governance and trust in the central platform operator – Enforcement and access control is done via the central platform	– Requires strong alignment but allows greater autonomy and fewer risks – Each participant retains enforcement and access control	– As participants retain autonomy on the level of data shared, benefits need to be proportional to the shared data

CASE STUDY 10

Ordos-Envision Net-Zero Industrial Park | operationalizing multistakeholder data governance at the cluster scale

The Ordos-Envision Net-Zero Industrial Park in Inner Mongolia, China, illustrates how cluster-level data governance can support coordinated energy optimization and carbon management across multiple independent organizations.

The initiative connects industrial facilities, energy assets and public management entities via a shared digital platform that enables cross-company monitoring, analysis and coordination of energy use and emissions across more than 50 industrial enterprises. AI-based optimization coordinates wind power, solar generation, energy storage and industrial demand, enabling collaborative energy management and demand response across the cluster.

To support this collaboration, Ordos established a structured governance model that combines institutional arrangements, contractual frameworks and digital infrastructure. A park-level data sharing and use agreement defines the roles, responsibilities and conditions for data exchange, while a centralized artificial intelligence of things (AIoT) platform implements these rules through technical controls.

Governance is organized through a multistakeholder structure. The Smart Park Management and Service Center functions as the central governance and coordination body, responsible for digital operations, facility management, enterprise services and overall data governance. An operational entity equivalent to a data governance office – composed of technical and operations personnel from Envision and the Park Management Committee – supports day-to-day implementation, including executing governance policy, managing data access, and monitoring data security and quality.

Specific responsibilities are distributed across participants. The Park Management Committee – representing the local government – provides regulatory oversight, funds the platform as shared public infrastructure and acts as a neutral orchestrator – convening stakeholders, resolving disputes through policy tools such as financial incentives, differentiated tariffs and green finance support, and serving as the arbitrator in cases of data misuse or contract breaches. Envision serves as the platform builder and operator, responsible for technical implementation, platform operations and enabling data exchange between enterprises. Industrial participants contribute data, participate in governance processes, and help shape collaboration rules while benefiting from shared insights and optimization capabilities.

The model combines centralized coordination with enterprise-level control. Data ownership remains with the participating companies, and sensitive and raw operational data is retained locally. Companies only share aggregated or non-sensitive data through the central platform. Standardization is applied at both the enterprise and platform levels: companies perform initial data preparation and quality validation before uploading data, while the platform applies shared semantic models, interface specifications and secondary validation processes to ensure interoperability among participants with varying levels of digital maturity.

Governance and technical mechanisms manage access control: participating companies define their own data-sharing scope and permissions, the Park Management Committee establishes security and compliance requirements and Envision implements the technical access control framework and platform-level enforcement mechanisms.

Through coordinated optimization and shared data visibility, the park has achieved approximately 80% on-site green electricity consumption while reducing overall energy costs by around 10%.

Source: Envision.

> **The future of net-zero industry is not built by individual companies, but by connected ecosystems. In Ordos, we are demonstrating how data can enable this transformation – linking energy, industry and infrastructure through a shared platform, while ensuring trust, transparency and control for every participant. This is how we operationalize net zero at scale.**
>
> Lei Zhang, Founder and Chief Executive Officer, Envision Group

With governance in place, decision rights defined, incentives aligned and trust institutionalized, the question shifts from whether organizations can collaborate to whether their data can be used. That is the challenge data readiness addresses.

4.3 Data readiness

Data readiness translates governance principles into usable data. It manages data in a way that allows it to be discovered, understood, trusted and reused across organizational boundaries.

Data readiness is critical in industrial clusters because collaboration depends on organizations being able to interpret and use data consistently despite operating differently. Without this foundation, even well-governed data remains difficult to integrate and apply in practice.

To operationalize data readiness across heterogeneous environments, **clusters must establish four core capabilities**, as outlined in Figure 8.

FIGURE 8 **Data readiness capabilities**

Metadata management
Discoverability and visibility readiness

Participants must be able to understand what data exists, how it can be used and whether it is trustworthy. A shared metadata catalogue enables participants to discover, assess and request access to relevant data assets without exposing the underlying data itself. It also reduces data discovery time, improves trust through transparency of quality and lineage, and supports compliant data sharing.

In practice: developer portals providing structured access to data products and APIs alongside their associated metadata

Data classification
Access and control readiness

Participants must agree on how datasets are categorized according to sensitivity and permitted use. Classification determines what data can be openly shared, what must be aggregated or anonymized, and what must remain restricted. Classification rules are embedded into the data life cycle; datasets are labelled with classification metadata, with handling requirements and access permissions aligned to the assigned level.

Classification categories: open, shared, restricted, confidential

Data quality and life cycle management
Trust readiness

Shared data must remain trustworthy over time. Quality validation rules, monitoring processes, version management and life cycle controls ensure that data remains reliable as systems evolve and new participants join. Data quality is not a static index – it must be tracked over time, with clear metadata records indicating how and when it was measured, against agreed business rules and thresholds.

Five quality dimensions: accuracy, completeness, consistency, uniqueness, validity

Semantic alignment
Interpretability readiness

Organizations often use different terms, identifiers and structures for the same underlying concepts. What one company calls “Site A”, another may call “Terminal 3”. Establishing shared master data definitions, reference models and controlled vocabularies creates a common semantic baseline without enforcing uniform internal architectures.

Many standards already exist, the challenge is consistent mapping, alignment and application

Building on existing standards

Industrial clusters do not need new standards to enable data collaboration. Many domain-specific standards already exist, such as the International Electrotechnical Commission’s (IEC) IEC 61968/61970 – the Common Information Model (CIM) – for energy systems, which provides a shared semantic model for data exchange between utilities, grid operators and industrial participants. The challenge is not the absence of standards, but inconsistency in their implementation across organizations. As a result, data readiness depends less on creating new standards and more on applying existing ones while preserving organizational autonomy.

Data readiness depends less on creating new standards and more on applying existing ones while preserving organizational autonomy.

AI as data collaboration enabler

AI-enabled tools can support data integration by matching schemas and entities across heterogeneous systems and mapping business terms and identifiers to common vocabularies. They can also support data quality and enrichment by automatically tagging and documenting metadata, detecting anomalies such as missing values, duplicates and inconsistencies, and extracting structured information from reports, logs and technical documents.

TABLE 2 | **Data readiness across collaboration models**

Centralized	Federated	Hybrid
– Common definitions and data structures are in place – Differences in meaning and structure are resolved centrally, and data quality is typically overseen by a central governance function	– Data models can be different but are aligned through mapping at each participating organization – There are minimum interoperability requirements such as shared vocabularies – Each participant is accountable for the quality of what they publish	– Combine both approaches depending on the data shared

CASE STUDY 11

Catena-X | interoperability through shared data models and standards

A critical component of data readiness is interoperability: the ability to ensure that data can be consistently understood and used across organizational boundaries.

Catena-X shows how interoperability can be achieved across a large and heterogeneous industrial ecosystem. It describes itself as the first trusted, multi-tier data ecosystem for the automotive industry, reporting that through its local hubs in China, France, Germany, the US and other markets, it can potentially address around 7,000 companies.[17]

The automotive industry operates through highly fragmented global supply chains; thousands of companies generate and exchange data using different systems, formats and definitions. This fragmentation limits end-to-end visibility and makes it difficult to support cross-company use cases such as traceability, product carbon footprint reporting, digital product passport and quality management.

Rather than attempting to standardize internal systems or introduce a universal schema, Catena-X uses a combination of shared data models, standardized semantics and agreed interfaces. These define how data should be structured, described and exchanged, allowing each organization to interpret it consistently while maintaining its own internal architecture.

Catena-X presents data using standardized connectors and describes it using common semantic models, ensuring that it can be used across organizations. Data contracts further define how it can be accessed, linking technical interoperability with governance requirements. This approach creates a consistent "shared language" across the ecosystem. Instead of uniform systems, interoperability requires alignment – allowing heterogeneous information technology (IT) landscapes to interact while preserving organizational autonomy.

One example of the value of standardized data is improved quality management. In a BMW-led use case, Catena-X enabled error detection on average four months earlier and, through improved traceability, reduced the potential recall scope from 1.4 million vehicles to just 14.[18] A 2025 Accenture-Fraunhofer/Plattform Industrie 4.0 study[19] suggests that, if such data-space-enabled quality management were scaled across the three main German automotive companies, it could generate an aggregate uplift of earnings before interest and taxes (EBIT) of around €1.2 billion in a recall scenario and around €450 million in a production disturbance scenario.

4.4 Technology

Governance sets the rules and data readiness makes data usable – but neither produces value without technology that can enforce those rules and move that data at operational scale.

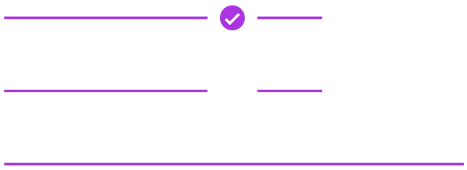
Technology provides the delivery mechanism for industrial data collaboration, not only connecting systems, but embedding trust, control and interoperability into how data is exchanged and used across organizations.

Regardless of the collaboration model, the underlying architecture can be presented in five layers. Figure 9 shows how data flows up through five "layers", from raw operational signals at the bottom to governed intelligence at the top, with each layer transforming or governing data before passing it on.

FIGURE 9 | Five architecture layers

Governed intelligence

L5 **Identity and access management (IAM), policy enforcement, audit**



Layer 5 · Control

Operationalizes governance decisions through technical enforcement

- Identity and access management (IAM) across organizational boundaries
- Role-based access controls (RBAC) and attribute-based access controls (ABAC)
- Policy enforcement, including who can access data, for what purpose, under which conditions
- Data use controls, monitoring, logging and audit

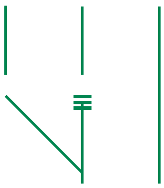
L4 **Dashboards, AI models, digital twins**

Layer 4 · Application

Where shared data is converted into operational and strategic value

- Cross-company dashboards and reporting tools
- AI and optimization models
- Digital twins for coordinated system-level decision-making
- Regulatory and compliance reporting solutions

L3 **Shared meaning, common vocabulary**

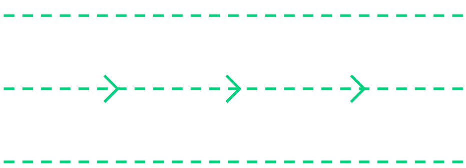


Layer 3 · Semantics and interoperability

Ensures data is interpreted consistently and reliably combined across organizations

- Shared data models and taxonomies
- Metadata catalogues enabling dataset discovery
- Data product definitions, including ownership, service-level agreements (SLAs), quality metrics
- Lineage tracking for traceability and auditability

L2 **Ingest, transform, store**

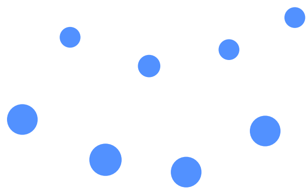


Layer 2 · Data plane

Ingests, transforms, stores and shares data across the cluster ecosystem

- Ingestion pipelines and streaming platforms
- Transformation frameworks aligning formats and schemas
- Storage systems, including data lakes or lakehouse platforms
- Query and orchestration services

L1 **Expose relevant data**



Layer 1 · Data sources

Selectively exposes relevant data from each company's environment

- Operational technology (OT), telemetry, IoT, manufacturing execution systems (MES), ERP and enterprise asset management (EAM) platforms
- Engineering models, sustainability systems, external feeds

AI increasingly enables the accommodation of more raw and unstructured data

Raw data enters

TABLE 3 | **Technology across collaboration models**

Centralized	Federated	Hybrid
– Data plane, semantic, application and control layers are all centralized into the central data platform	– Each participating organization operates their data plane, aligns data locally and publishes standardized metadata – Control is distributed across participants, requiring strong coordination	– Shared semantic services are in place, as well as centralized policy definition combined with local enforcement

CASE STUDY 12

Port of Singapore | enabling seamless data exchange across the maritime ecosystem

The Port of Singapore illustrates how a common, standards-based data and API exchange platform can transform digital connectivity across a complex, multistakeholder maritime ecosystem.

In maritime operations, data exchange between stakeholders – shipping lines, port authorities, agents, regulators and technology providers – has historically relied on bilateral, point-to-point integrations. Each connection required custom development, individual contracts and dedicated maintenance, resulting in an integration topology that grew in complexity with each new participant. As digital services expanded and cross-border reporting requirements intensified, integration costs and time became structural barriers to collaboration across the sector.

To address this, the Maritime and Port Authority of Singapore (MPA) launched OCEANS-X (Open/Common Exchange And Network Standardisation-eXchange) in April 2026 as a government-to-government and government-to-business digital platform. Rather than expanding the network of bilateral connections, OCEANS-X enables ecosystem partners to discover, access and share data seamlessly within a common environment. Participants can connect their systems to the platform, transmitting data directly to the MPA's digital systems – removing the need for portal-based, manual submissions.

In practice, OCEANS-X operates across several interlocking capabilities. Operational and reference data from across the maritime ecosystem – including vessel schedules, positions, port information, customs filings and bunker sales – is exposed through standardized APIs. The platform currently hosts over 100 APIs and datasets, handling both static reference data and dynamic operational feeds.

In addition to data sharing, OCEANS-X supports transaction flow between systems. For example, through the "port clearance as a service" suite of APIs, technology solution providers and companies can integrate their systems with MPA's digital services, such as digitalPORT@SG™, to submit port clearance applications when calling at the Port of Singapore. Industry players and start-ups are welcome to develop, integrate and deploy new services on the platform, including analytics and AI-enabled tools. The platform manages access through authorization controls that govern which participants can discover and use each API.

The early indicators of value reflect the impact of this architecture. The port clearance API is projected to reduce processing time by up to 100,000 work-hours annually. This points to a broader pattern with OCEANS-X: a well-structured, interoperable platform can lower the cost of adding new participants and services over time, shifting data collaboration from a one-off project towards shared infrastructure.

Source: Maritime and Port Authority of Singapore.

> **No single carrier, port or terminal operator can optimize global supply chains alone. When shipping lines, ports, logistics partners and industrial players share the right data at the right level of trust, everyone plans better – fewer delays, less wasted fuel, more resilient routes. That is the opportunity ahead for our industry.**
>
> Takeshi Hashimoto, Chairman, MOL

A well-designed technology architecture reduces the marginal cost of adding new participants and use cases. However, every new participant and data connection expands an ecosystem's attack surface. As its data infrastructure becomes more interconnected and operationally critical, the question of how to protect it and keep it functioning when compromised becomes inseparable from the question of how to build it. That is what cyber resilience addresses.

4.5 Cyber resilience

78%

of chief executive officers (CEOs) of highly resilient organizations identify supply chain and third-party dependencies as the most significant cybersecurity challenge.

According to the *Global Cybersecurity Outlook 2026* survey, 78% of chief executive officers (CEOs) of highly resilient organizations identify supply chain and third-party dependencies as the most significant cybersecurity challenge.[20]

In interconnected industrial clusters, where companies are physically co-located, share infrastructure and are often part of the same supply chains, these dependencies are even more concentrated. A weakness in one participant can propagate across the ecosystem, affecting shared operations, data integrity and trust. The requirement is not only to secure clusters against cyberattacks but also to ensure resilience when attacks are successful.

Cyber resilience is the ability of an industrial system to minimize the end-to-end impact of cyber incidents and continue operating in adverse conditions. Just as an immune system protects and stabilizes the human body, cyber resilience strengthens the entire ecosystem by ensuring that critical functions can withstand disruption, recover quickly and adapt over time.

While cybersecurity focuses on preventing attacks and protecting systems, cyber resilience assumes that breaches are inevitable in complex, interconnected environments. This shift is particularly important in industrial clusters and industrial ecosystems. As digital and physical systems converge, and organizations become more interdependent, absolute protection is unrealistic. What matters instead is whether the cluster can maintain critical operations, coordinate response across participants and strengthen its defences over time.

Cyber resilience across the cyber incident life cycle

Cyber resilience in industrial clusters requires coordinated action across the full incident life cycle: before, during and after cyber events.

FIGURE 10 | **Cyber resilience across the cyber incident life cycle**

Source: World Economic Forum. (2024). *Unpacking Cyber Resilience*. https://www.weforum.org/publications/unpacking-cyber-resilience/.

Cyber resilience is strongest when security is designed into the operating model rather than applied as an afterthought.

Before (preparedness)

The focus is on reducing exposure and aligning baseline capabilities across participants: identifying shared critical assets and interdependencies, defining a minimum cybersecurity baseline and establishing common rules for third-party systems and integrations. It requires embedding security-by-design into new systems and data-sharing mechanisms to minimize risk.

During (response)

The focus is on speed, coordination, and containment: participants share real-time threat signals, trigger coordinated response playbooks, and escalate incidents quickly and consistently across organizations, leading to faster containment and a reduced risk of disruptions propagating across interconnected systems.

After (recovery and learning)

The focus is on restoring operations and strengthening resilience. Critical services are restored in a coordinated manner, while root causes and lessons learned are shared across participants. Insights are fed into updated standards, improving response mechanisms and strengthening collective resilience over time.

AI is a critical defensive enabler across all three phases: supporting threat modelling and vulnerability scanning before an incident; augmenting detection, containment and triage during response; and accelerating root cause analysis and strengthening shared defences after.

Operationalizing cybersecurity at the cluster level

Cyber resilience is strongest when security is designed into the operating model rather than applied as an afterthought. For industrial clusters and industrial ecosystems, this means embedding security-by-design across the same three dimensions that enable data collaboration.

In data governance, cyber resilience requires explicit accountability for cyber risk across shared digital infrastructure, with cluster governance bodies treating it as an agenda item alongside value and technology decisions, given that the consequences of incidents are inherently ecosystem-wide. Governance decisions of incremental connections should also weigh the benefits against the cost of increased cyber risk exposure.

In data readiness, cybersecurity requirements should be embedded in shared standards so that participation does not create uneven exposure across the ecosystem.

In technology, security-by-design must be operationalized directly into the technology stack. It also means applying data minimization to device telemetry: organizations should only contribute data to shared pools where it directly feeds an active, tracked use case.

CASE STUDY 13

Port of Los Angeles | building ecosystem-wide cyber resilience through shared threat intelligence

As port ecosystems become increasingly digitized, cybersecurity risks extend beyond individual organizations to the entire supply chain. At the Port of Los Angeles, increasing reliance on digitally controlled systems, interconnected IT and operational technology (OT) systems, and real-time data exchange significantly increased the port's exposure to cyberthreats. The volume of attempted attacks grew rapidly – from around 10 million to over 100 million per month – underscoring the scale and systemic nature of the risk.

While the port had already established a Cyber Security Operations Center (CSOC) to protect its internal infrastructure, it became clear that this approach was insufficient in a highly interconnected environment. Many critical processes – such as cargo handling and logistics coordination – depend on external stakeholders, including terminal operators, trucking companies, railroads, shipping lines and utilities. A cyber incident affecting any one of these actors could disrupt the entire port ecosystem.

To address this, the Port of Los Angeles established in 2022 the Cyber Resilience Center (CRC), a dedicated platform for ecosystem-level cybersecurity collaboration. Operating as a public-private partnership, the CRC brings together more than 1,000 stakeholders to share threat intelligence and coordinate responses across the port community. Its core function is to provide an operational view of cyber risks and serve as an early warning system that improves the speed, quality and reach of information-sharing across the ecosystem.

The CRC operates as a non-invasive coordination layer, complementing rather than replacing existing cybersecurity systems in participating organizations. Companies retain control over their infrastructure and data while contributing selected information through channels ranging from automated interfaces to manual reporting. This flexible approach enables organizations at varying levels of digital maturity to participate without exposing sensitive data or disrupting their operations.

At the operational level, the CRC monitors and correlates cyber events across the ecosystem, producing threat intelligence reports and alerts that it shares with participants. By aggregating signals from multiple sources, it detects emerging threats sooner and provides actionable guidance tailored to port operations. In addition, it supports training, awareness and coordination activities, helping build a shared understanding of risks and response strategies among stakeholders.

The value of this approach lies in its ability to transform fragmented cybersecurity practices into a coordinated, ecosystem-level capability. The CRC enables collective defence, where insights from one participant can strengthen the resilience of all. The initiative's impact is reflected in reduced exposure to systemic disruptions, improved preparedness and the enhanced continuity of critical operations across the port.

Source: Port of Los Angeles.

> **Cybersecurity is no longer an individual company challenge – it's a supply chain challenge. The Cyber Resilience Center gives our port community a common operating picture of emerging threats, helping stakeholders share information, respond faster and strengthen the resilience of the critical systems that keep cargo moving.**
>
> Gene Seroka, Executive Director, Port of Los Angeles

Conclusion

Data collaboration is a critical enabler of value creation in the intelligent age. Unlocking the full potential of advanced digital technologies depends on the ability to share and use data across organizational boundaries in a trusted, scalable and secure way. Yet, structural, organizational and technical barriers continue to limit progress.

Industrial clusters provide a unique environment for addressing these challenges and unlocking tangible value. Their concentration of interconnected actors, shared infrastructure and operational interdependencies creates strong opportunities for system-level optimization – from energy and resource efficiency to logistics, resilience and new business models. As such, **clusters can serve as practical testbeds for developing, validating and scaling data collaboration approaches that can then be applied to other industrial ecosystems**.

Importantly, data collaboration is not a one-time effort but a continuous process. As initial use cases go live and demonstrate value, they create the foundation for broader participation, additional applications and ongoing innovation. This phased approach reduces complexity, builds trust incrementally and enables ecosystems to scale over time.

The case for action is clear:

- **Business and government leaders should start now** with value-led initiatives that solve tangible operational or commercial challenges, build trust among participants and demonstrate a credible path to scale. The objective should not be to accumulate pilot projects but to establish scalable, commercially viable models capable of sustaining long-term participation and innovation.

- **Industrial clusters should actively shape the policy environment** that enables collaboration. Particularly where data sharing serves a wider public interest, clusters are well positioned to inform policy discussions on data access, interoperability standards, cybersecurity requirements and the responsible application of AI in industrial environments – helping translate on-the-ground experience into frameworks that accelerate adoption more broadly.

- **Organizations should exchange learnings and best practices**. Sharing governance models, implementation lessons and practical experience across the wider community of clusters can help replicate what works, avoid repeated friction and accelerate the shift from isolated experimentation to systemic impact.

The World Economic Forum offers business and government leaders the opportunity to work with the Transitioning Industrial Clusters (TIC) community to translate the lessons in this report into shared governance models, policy frameworks and scalable collaboration architectures that can drive intelligent industrial transformation across ecosystems.

Contributors

Lead authors

Filippos Kaponis
Managing Director, Accenture

Nicola Mackow
Strategy Manager, Accenture

Irene Varoli
Lead, Transitioning Industrial Clusters, World Economic Forum

Acknowledgements

The World Economic Forum would like to extend its gratitude to the following individuals for their valuable contributions to this report. The report does not necessarily reflect the views of these individuals and/or their organizations. Expert advice is purely consultative in nature and does not imply any association with the takeaways or conclusions presented within this report.

Manuel Romero Agudo
Cybersecurity Architect, Repsol

Amin Aljaber
Chief Information Officer, Nesma & Partners

Daniel Alvarez-Gomez
Cybersecurity Lead, Hitachi Energy

Chiara Barbeschi
Specialist, Technology and Innovation, World Economic Forum

Maria Basso
Head, AI Applications and Impact, World Economic Forum

Filipe Beato
Manager, Technology and Innovation, World Economic Forum

Thomas Blood
Principal Strategic Adviser, Enterprise Transformation, Amazon Web Services (AWS)

Gary Boyle
Principal Director, Accenture

Tomaz Brentano
Environmental Specialist, Prumo Logística

Federico Capaccio
Specialist, Applied AI, World Economic Forum

Mathias Larsson Carlander
Strategy Officer, Traton Group Research & Development, Traton

Dimitris Christopoulos
Professor of Systems Analysis, Edinburgh Business School, Heriot-Watt University

Maximilian Dauer
Project Manager, Siemens

Chris Davies
Senior Director, DP World

Jacky Fox
Senior Managing Director, Accenture

Nicolas Gavela Martinez
Industry and Circularity Decarbonization, Moeve

Ginelle Greene-Dewasmes
Initiatives Lead, Artificial Intelligence and Energy, World Economic Forum

Glenn Gu
Product and Development Senior Director, Envision

Victor Guang Shi
Supply Chain Resilience Lead, Advanced Manufacturing Research Centre, University of Sheffield

Rana Hajirasouli
Founder and Chief Executive Officer, The Surpluss

Jon Hall
Technical Lead for Connected Factories, Advanced Manufacturing Research Centre, University of Sheffield

Ryan Hardin
Head of Unit, Energy Transition, MYCentre4IR

Puneet Harminder Singh
Vice-President, Technology and Innovation for Electrification and Automation, Siemens

Magnus Hellqwist
Director, Shared IT Services, Scania

Yannick Herrbaut
Chief Information Security Officer, Port of Antwerp-Bruges

Nuttavut Intarode
Sustainable Development Director, Siam Cement Group

Nigel Jenvey
Vice-President, Carbon Capture Utilization and Storage (CCUS) and H_2 Project Development, Baker Hughes

Devendra Jain
Initiatives Lead, Frontier Technologies for Operations, World Economic Forum

Eduardo Kantz
Executive Director, Public Affairs, Prumo Logística

Can Kaymakci
Head of Coordination SynErgie, Fraunhofer Institute

Alex Korovkin
Head of Cybersecurity, Consolidated Contractors Company (CCC)

Tracy Leslie
Lead, Net Zero Industrial Clusters, Electric Power Research Institute

Thomas Leurent
Co-Founder and Chief Executive Officer, Akselos

Jun Jie Lim
Senior Manager, Maritime Digital Capability, Maritime and Port Authority of Singapore

Emilio Lomelin Rodriguez
Digital Lead, Advanced Manufacturing Research Centre, University of Sheffield

Epco Maat
Data Governance Senior Manager, Accenture

Stephen McGurk
Founding Director, Circular Ecosystems

Sandra Melki
Vice-President, Marketing and Sustainability, Technip Energies

Sophie Miremadi
Vice-President, Global Government Affairs and Public Policy, AVEVA

Piotr Misiewicz
Technology Strategy Manager, Accenture

Per Møller
Senior Special Adviser, Kalundborg Symbiosis

Sascha Müller
Customer Executive and Member of Management, Northern Europe, DNV

Catherine O’Brien
Managing Director, Accenture

Jackie O’Dowd
Chief Executive Officer, Realising-Potential

Charles Pacini
Manager, Transforming Industrial Ecosystems, World Economic Forum

Seshanka Palukuri
Group Strategy Lead, Greenko

Geoffrey Parker
Professor, Thayer School of Engineering, Dartmouth College

Kumar Patchigolla
Professor of Decarbonization of Industrial Clusters, Teesside University

David Prats
Vice-President, Data Risk and Security, Schneider Electric

Shadi Rafeh
Manager, Management Information System and Digitalization, Consolidated Contractors Company (CCC)

Tracy Rucinski
Head, International Corporate Affairs, Moeve

Jörgen Sandström
Head, Transforming Industrial Ecosystems, World Economic Forum

María San Salvador del Valle
Strategic Initiatives, SPRI Group, The Basque Business Development Agency

Marijn van Schoote
Ferm Managing Director, Port of Rotterdam

Yuriy Shaulko
Global Cloud Security Chief Technical Officer, Trafigura Group

Edmund Sim
Assistant Director, Digital and Data Science Division, Maritime and Port Authority of Singapore

Douwe van der Stroom
Programme Manager, Smart Energy and Industry, Port of Rotterdam

Chandrima Thomin
Specialist, Transitioning Industrial Clusters, World Economic Forum

Konstantinos Trantopoulos
Adviser and Research Fellow, International Institute for Management Development (IMD) Business School

Leonardo Vannozzi
Strategy Analyst, Accenture

Sheeba Varughese
Director of Information Technology and Chief Information Officer, Port of Los Angeles

David Villaseca
Chief Digital Officer and Chief Strategy Officer, Moeve

Michael Wade
Professor of Innovation and Strategy, Cisco Chair in Digital Business Transformation, International Institute for Management Development (IMD) Business School

Calvin Woo
Director, Digital Transformation, MyDigital

Ulvi Zamanbayov
Data Science Lead, Caspian Innovation Center, State Oil Company of the Azerbaijan Republic (SOCAR)

Dylan Zhang
Research and Development Director, Green Partnership of Industrial Parks (GPIPC)

Production

Laurence Denmark
Creative Director, Studio Miko

Charlotte Ivany
Designer, Studio Miko

Will Liley
Editor, Studio Miko

World Economic Forum Public Engagement

Maxwell Hall
Creative Editorial Lead

Floris Landi
Design Lead

Gayle Markovitz
Head, Written and Audio Content

Sybile Penhirin
Head, Video and Design

Endnotes

1. World Economic Forum. (2025). *Five Steps for Digital Collaboration in Industrial Clusters*. https://reports.weforum.org/docs/WEF_Five_Steps_for_Digital_Collaboration_in_Industrial_Clusters_2025.pdf.
2. World Economic Forum. (2026). *Intelligent Infrastructure: A Primer*. https://www.weforum.org/publications/intelligent-infrastructure-a-primer/.
3. Ministry of Industry and Information Technology of the People's Republic of China. (2026). *Notice from Eight Departments on Issuing the "Implementation Opinions on the Special Action of 'Artificial Intelligence + Manufacturing'"*. https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2026/art_01010414608a4226b30687773bb21bdf.html.
4. Chakraborty, A. (2025). *The Data Value Gap: Why Only 32% of Companies Realise Tangible Benefits from Data*. Medium. https://theblueowls.medium.com/the-data-value-gap-why-only-32-of-companies-realise-tangible-benefits-from-data-e5d52d6c051c.
5. World Economic Forum. (n.d.). *System Value*. https://www.weforum.org/projects/system-value/.
6. European Commission. (2022). *Data Act: Commission proposes measures for a fair and innovative data* economy. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.
7. Community insights were derived from senior multistakeholder experts engaged through six in-person and virtual workshops conducted globally by the World Economic Forum in 2025–2026, and from one-to-one consultations.
8. Eurostat. (2026). *E-business integration*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-business_integration.
9. Accenture. (2025). *State of Cybersecurity Resilience 2025*. https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/State-of-Cybersecurity-report.pdf.
10. Security Scorecard. (2025). *2025 SecurityScorecard Global Third-Party Breach Report*. https://securityscorecard.com/wp-content/uploads/2025/03/SSC-Third-Party-Breach-Report_031225_03.pdf.
11. Accenture. (2024). *Securing the Digital Core in the Gen AI Era*. https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/Accenture-Securing-The-Digital-Core-In-The-Gen-AI-Era.pdf.
12. World Economic Forum. (2025). *Advancing Responsible AI Innovation: A Playbook*. https://reports.weforum.org/docs/WEF_Advancing_Responsible_AI_Innovation_A_Playbook_2025.pdf.
13. World Economic Forum. (n.d.). *System Value*. https://www.weforum.org/projects/system-value/.
14. Gabellini, M., Civolani, L., Ronchi, M., Naldi, L. D., et al. (2025). Data Spaces in Manufacturing and Supply Chains: A Review and Insights from European Initiatives. *Applied Sciences*, vol. 15, issue 11. https://www.mdpi.com/2076-3417/15/11/5802.
15. Contractual and technical safeguards can limit misuse, but they cannot eliminate the underlying exposure.
16. Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., et al. (2021). Advances and Open Problems in Federated Learning. *Foundations and Trends in Machine Learning*, vol. 4, issue 1. https://arxiv.org/pdf/1912.04977.
17. Catena-X. (2025). *Catena-X Your Automotive Network: General Introduction*. https://catena-x.net/wp-content/uploads/2025/05/Catena-X-General-Introduction-Presentation-1.pdf.
18. Catena-X. (n.d.). *Driving quality together: how OEMs and suppliers transform quality management with Catena-X*. https://catena-x.net/success-stories/quality-management/.
19. Bongardt, S., Falk, S., Guggenberger, T., Hamper, A., et al. (2025). *The Monetary Value Added By Data Spaces*. Plattform Industrie 4.0. https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/2025-i40-monetary-value-added-of-data-spaces.pdf?__blob=publicationFile&v=6.
20. World Economic Forum. (2026). *Global Cybersecurity Outlook 2026*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf.

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum is the trusted global platform for public-private cooperation, bringing together leaders from business, government, civil society, international organizations, academia and the next generation to turn foresight and dialogue into meaningful action on the world's most pressing challenges.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org