Chapter 29
From Linear Supply Chains to Open Supply Ecosystems

Fabian Biegel and Nemrude Verzano

Abstract The 2020s will be the beginning of an "Age of Data." Data will help us unleash huge potentials in private but particularly also in the industry. At the same time, partly driven by the availability of this real-time information, the customer-supplier relationships are transforming from linear supply chains into networks and data-driven ecosystems. Efficient standards and technologies are key to this transformation.

However, the biggest hurdle to sharing data continues to be the lack of trust in secure, transparent, and trustworthy information exchange. Concepts and instruments like the International Data Spaces are essential to guarantee data sovereignty.

The SAP Asset Intelligence Network is therefore complemented by the core elements of IDS to maintain trust and transparency throughout the entire industry value network.

29.1 Introduction

Forbes has proclaimed the 2020s the "Age of Data." The EU Commission forecasts a tripling of the value of the European data economy in the next 5 years. McKinsey and PwC assess the market potential enabled by data at around US$13-16 trillion by 2030. Or, to take it beyond financials: Open data could reduce malaria mortality rates by up to 92%, saving up to 400,000 people a year from death. So, we know about the value of data and the exchange and sharing of data in particular.

However, the biggest hurdle to sharing data—in addition to technical problems, capital expenditure, and lack of skills—continues to be the lack of trust in secure, transparent, and trustworthy data ecosystems.

Mechanisms and tools are needed to address this deficiency in trust, in particular for business-to-business scenarios where we share sensitive or even confidential information. We find such a tool in the International Data Spaces.

F. Biegel (✉) · N. Verzano
SAP SE, Walldorf, Germany
e-mail: fabian.biegel@sap.com; nemrude.verzano@sap.com

B. Otto et al. (eds.), *Designing Data Spaces*,
https://doi.org/10.1007/978-3-030-93975-5_29

29.2 Data at the Center of Industrie 4.0

The digital transformation of the manufacturing sector took hold early on with the proclamation of the fourth industrial revolution in 2013. Industrie 4.0 even places the availability of data at the center of its definition[1]:

Industrie 4.0 has its foundation in the 'availability of all relevant information in real time through the networking of all entities involved in the value chain and the ability to use the data to optimize the value added at any given time.'

Looking at the business impact of data for Industrie 4.0, the PAiCE study by the German Federal Ministry for Economic Affairs and Energy[2] estimates, for instance, that artificial intelligence has the potential to contribute one-third of the total growth of the manufacturing industry and thus a gross value added of over 30 billion euros within 5 years. In particular, applications for predictive analytics, intelligent assistance systems, robotics, intelligent automation, and intelligent sensor technology offer the greatest opportunity.

Not yet at the center of attention, but already being recognized as potential disruption of the established collaboration models and gaining in importance in recent years, is the breaking up of traditional supply chains in favor of digital platforms[3] and agile networks[4] of business partners in continuously changing roles.[5]

Not least, these will form the core of Industrie 4.0: dynamic ecosystems that make information their central asset not only for optimizing traditional production processes but rather for embarking on new, expanded business models based on data and artificial intelligence.

However, this requires a comprehensive approach to building these industrial data spaces based on efficient tools and standards for manufacturing data ecosystems to thrive.

29.2.1 Data Ecosystems and Data Spaces

Traditional supply chains have proven efficient and robust over decades of industrial production. Disruptions to very linear supply chains however, such as the Eyjafjallajökull eruption in March 2010, low water levels (2019) in the river Rhine, or more recently the COVID-19 pandemic, have shown how fragile they

[1] Umsetzungsstrategie Industrie 4.0, Plattform Industrie 4.0, 2015.

[2] Potenziale der Künstlichen Intelligenz im produzierenden Gewerbe in Deutschland, iit – Institut für Innovation und Technik, 2018.

[3] Wertschöpfung durch digitale B2B-Plattformen, Plattform Industrie 4.0, 2020.

[4] Collaborative data-driven business model, Plattform Industrie 4.0, 2020.

[5] Value Networks as the Foundation for Digital Business Models, Platform Industrie 4.0, giz and CCID, 2020.

also are. German carmakers were still producing at the same volume at the start of the COVID-19 pandemic in spring 2020, while northern Italy—and thus key suppliers to the industry—had already been hit hard and were no longer able to meet their supply commitments. This led to significant interference in the production schedule. Automotive manufacturers experienced similar disruptions in 2021 when major chipmakers were unable to supply according to plan due to extraordinarily high demand from the better-paying consumer electronics industry.

Now, suppliers can't be easily exchanged when it comes to complex parts like in the automotive industry. Digitization and frequent information exchange however can help adopt resource and production planning with very low latency and react at an early stage making the supply chain more resilient to external disruptions. This is especially true if comprehensive information networks with direct information flow between parties at all levels of the supply chain can eliminate gatekeepers that previously impeded the flow of information.

While these data networks enable dynamic data exchange between peers, forming actual data spaces holds even greater opportunities for the partners. The use of Big Data in the industry for optimization, for instance, or AI-based algorithms for dynamic (or even predictive) asset management requires building application-specific, virtual data pools for analytics and machine learning beyond the one-to-one data exchange for transactional purposes.

Even more important for data networks and data spaces than in linear customer-supplier relationships, however, are trust in the partners involved and the appropriate handling of business-critical data. Thus, we heavily rely on the right tools to guarantee data sovereignty.

29.2.2 Standards

Business networks and ecosystems that build their core around information and data depend on finding interoperability concepts, common languages, ontologies, rules, and standards to exchange this information efficiently and use it effectively.

The benefits of such data ecosystems follow the mechanisms of classical network economics: the potential value of an existing network with *n* established network members increases—to put it simply—exponentially with each new partner.[6] But this also means that size, growth, and efficiency in the exchange of information are the keys to success. Easy onboarding of new members and their eventual offboarding with low hurdles and reliable, established standards are core to this effort.

Technical communication standards and architectures like MQTT messaging or OPC UA have been core to industrial data exchange for a decade. Same holds true

[6]For example, by 2n + 1 applying Metcalfe's law as first described in Metcalfe's Law and Legacy, George Gilder, 1993.

for semantics and ontologies like ECLASS or the NAMUR data model. In recent years, the demand for complex industrial data spaces has been added, which realize a comprehensive view of each asset in the form of a digital twin that covers the entire life cycle up to the recycling aspect in a circular economy. The Asset Administration Shell is one result of these efforts.

29.2.3 Trust and Security

As cited at the beginning, the biggest hurdle to widespread transformation to industrial business networks is trust in network partners and, perhaps even more so, in reliable, secure technology tools that technically underpin this trust.

Especially in data-intensive partner consortia, guaranteeing one's own data sovereignty is inviolable: the ability to not only monitor but actually control at all times where and how "my" data is stored and processed—but even more so, which third parties can access this data and whether it is handled according to the previously agreed terms.

While decentralized concepts such as *Linked Data* and *SOLID* from Tim Berners-Lee and the Massachusetts Institute of Technology are increasingly gaining recognition in the private sector, we see the International Data Spaces at the forefront of these efforts in the area of industrial applications and the "gold standard" for the trustworthy exchange of business information.

However, trust needs to be established throughout the entire technology stack which on the one hand side includes technical security of any data exchange infrastructure and Cloud service involved but also operational aspects and legal framework conditions.

Europe's GAIA-X initiative for a trustworthy federated data and cloud infrastructure is aimed to design and implement an infrastructure ecosystem that meets these requirements. Along with IDS's data sovereignty concepts and toolset, GAIA-X provides a comprehensive reference design and policy framework to underpin these ambitions for innovative yet trusted data ecosystems.

29.3 SAP Asset Intelligence Network

As being described above, the challenges of decentral infrastructures and business applications are not limited to technical challenges, but especially valid to compliance and regulatory aspects. One of the emerging areas is asset management to address the maintenance, operation, and further services that are relevant to an asset or rather device or machine. While real-time transparency is important for specific applications, new business models can also be realized with an efficient asset management. Therefore, the exchange of consistent and interoperable master,

Fig. 29.1 Traditional exchange of master data (©2021, SAP)

transactional, and unstructured IoT data is getting increasingly important to many companies, regardless of the tools from different vendors that are being used.

The traditional way of data exchange is being depicted in Fig. 29.1 and has turned out to be impractical in many ways to enforce collaboration within a company and externally with suppliers or service providers. In many cases, time-consuming processes are in place to on- and offboard partners, service providers, and even employees of the same company because of the heterogeneous applications and tools in the IT landscape of a company. Real-time and sensitive data of assets are difficult to share and need a lot of effort and approvals. Often enough, data is being shared by email.

SAP addressed these challenges since several years already and provides the solution SAP Asset Intelligence Network (AIN), which simplifies cross-company collaboration and consolidates asset-oriented activities from operation over maintenance up to machine learning-driven services like predictive maintenance. Different stakeholders are able to access asset information at a central place to get a transparent overview about the current status and the history of all activities that are stored in different backend systems. Spare part ordering can also be organized, or firmware updates made available, and operators notified. Based on assigned user profiles, the access to data and information can be managed and limited—see Fig. 29.2.

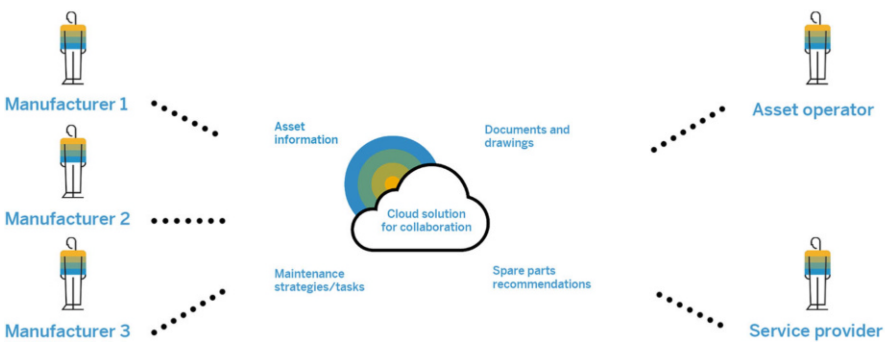

Fig. 29.2 SAP Asset Intelligence Network allows cross-company collaboration and provides transparency of the asset (©2021, SAP)

AIN is being used to store the digital twin of an asset. As soon as the unique asset has been produced and serialized, the digital twin can be onboarded in AIN.

29.4 Data Governance with IDS

The asset management organized in a centralized manner like AIN helps many companies create transparency of an asset and enforce collaboration. From documents like CAD files and manuals, over current IoT data, up to maintenance strategies, AIN enables every stakeholder to access relevant data centrally. But why adding a de-centralized approach like IDS to a well-functioning environment? This article is meant to emphasize that established mechanisms can be extended with new approaches without disrupting the running and existing processes. Usually, existing IT applications are not being turned off to introduce new features or capabilities but transition phases being preferred instead.

As described, AIN already provides data access capabilities to enforce collaboration across companies, but this traditional kind of user management is not sufficient to cope with data being stored at different places on different cloud or edge platforms. Especially IoT data that need to be processed by service providers cannot be governed in a manner that the usage and the processing of the provided data are being controlled.

Current data sharing approaches are limited and cannot sufficiently cover all requirements that have been partly described above to support a scalable enterprise usage. IDS allows data governance if needed and can enrich existing sharing features of AIN to improve the collaboration. Especially a controlled data space, where unstructured IoT data of the assets need to be shared with different stakeholders, will help many companies overcome machine learning relevant challenges to manage data access and to monitor how a trusted consumer is processing the data. For example, lengthy procedures to get IoT data to a machine learning service provider and monitor the exchange between the stakeholders can be dramatically improved by using IDS components. While the compliance and commercial aspects are being managed by the Clearing House, access to the data is being managed by an IDS Connector. How data is being processed depends on the scenario and respective data apps that will be running in a connector. Once the processing of the data is done, the results can be transferred by the IDS Connector as well. The predictive maintenance feature of AIN can be enriched with IDS capabilities to organize and monitor data exchange in a much more compliant manner.

The example above shows how IDS can enhance an existing application and its sharing features with data governance capabilities (Fig. 29.3). There are more potentials to apply IDS to existing and established business scenarios. Pay per use of assets, collective intelligence, and governance of documents are just some to mention that would benefit from the IDS approach.

Fig. 29.3 Enhancement of an existing application with IDS capabilities (©2021, SAP)