
# The Industrial Data Space

## A Cloud Based Approach

A Polestar & Nexor Whitepaper

# Exec Summary

*The industrial data space (IDS) is a virtual data space leveraging existing standards and technologies, as well as accepted governance models for the data economy, to facilitate the secure and standardised exchange and easy linkage of data in a trusted business ecosystem. It thereby provides a basis for smart service scenarios and innovative cross-company business processes, while at the same time making sure data sovereignty is guaranteed for the participating data owners*[1].

Ever since the industrial revolution changed the way we manufacture goods, Operational Technology (OT) has been the key enabler of both the processes required to produce those goods, and the creation of the supply chain industry needed to support their production.

Fast forward to today and technology now allows mass production to occur at a scale capable of meeting global demand. However, to fully realise their potential, companies need their OT to be able to share data, for analysis and control, in real time. This is where Information Technology (IT) comes into play. IT allows data to be shared easily and securely over networks for access by those who need it, but to utilise this data a viable method of connecting IT to OT is required. The Industrial Data Spaces Association aims to plug this gap by proposing an efficient and standardised way of connecting OT and IT systems, thereby avoiding the variety of serious complications that can, by default, arise when trying to link the two together.

In an ideal world these systems (which are separated by business function), would still be able to easily and effectively share data with each other. However, when it comes to putting this into practice it is nearly impossible to circumvent the fundamental differences that exist between OT and IT systems, and their respective operators. Companies that can identify and seek to bridge this gap within their organisations and their external supply chains could reap massive benefits from the implementation of a solution to these problems. This paper, based on an interpretation of the IDS Reference Architecture Model v2[2] further explores the possibility of utilising cloud services as de-centralised proxies between different stakeholders, eliminating the need for direct interactions or expensive integration between disparate systems. Potential upsides of this include; increased speed to market for new products / services, lowering the cost of production, reducing friction between organisational silo's and mitigating possible security risks.

1. Auer, S., Cirullies, J., Jürjens, J., Menz, N., Schon, J. and Wenzel, S. (2016). White paper Industrial Data Space. [online] Available at: https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/whitepaper-industrial-data-space-eng.pdf
2. REFERENCE ARCHITECTURE MODEL. (2019). [online] Available at: https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/IDS-Reference-Architecture-Model.pdf



# OT and IT – dysfunctional siblings

From an information security perspective OT and IT seem incompatible at a base level. For instance, IT is concerned with the Confidentiality, Integrity and Availability (CIA) of data; data is inaccessible to those without clearance, data is consistent and accurate, and finally everyone who should have access can access it when they need to. OT on the other hand has a completely different set of priorities and the concerns are reversed, i.e. the Availability, Integrity, Confidentiality (AIC) of data. One of the main reasons for this is due to the exorbitant cost to the business if Industrial Control Systems (ICS) are down for extended periods of time. Other important concerns for OT are reliability and safety, so the perspective is skewed towards a cyber-security, rather than an information-security approach.

Therefore, traditional methods of IT security are impractical if viewed through the CIA triad and in certain cases, simply impossible, particularly if you take into consideration, from a (cost-benefit analysis point of view) the application of security patches which is a 'Cyber Essential' for IT departments.

OT environments are highly customised at site level and rarely have duplicate systems on which to test new patches so production departments are hesitant to allow changes for fear of disruption, or unacceptable downtime while a change is made. These issues are further compounded by a lack of understanding from IT professionals as to the different needs of OT (with the emphasis on the 'Availability' of the CIA triad). A common mistake is problem identification by IT departments and then providing fixes based on their knowledge of making IT systems secure which does not sufficiently consider the impact this would have on the reliability and safety of machines. On the OT side, engineers can be nervous when connecting disparate systems into IT environments that are 'always being hacked' and may believe (falsely of course) that air-gap security is physically secure. This creates friction between IT & OT leading to an environment where cooperation for the benefit of the business falls by the wayside.

# Cloud and the Industrial Data Space

So how can Cloud technology and the Industrial Data Space (IDS) model overcome some of these barriers? One of the fundamental principles of sharing data is the assignment and mutual understanding of 'data ownership' (or Data Sovereignty). It's essential for the establishment of trust, which in turn, enables confidence and therefore allows business transactions to take place.

Without this built in concept, businesses will not allow their data to be sent into the IDS as through doing so, they would lose control over who can access it. With this concern in mind, there are five key roles set out within the IDS architecture which contribute to the management and utilisation of shared data.

**These are as follows:**

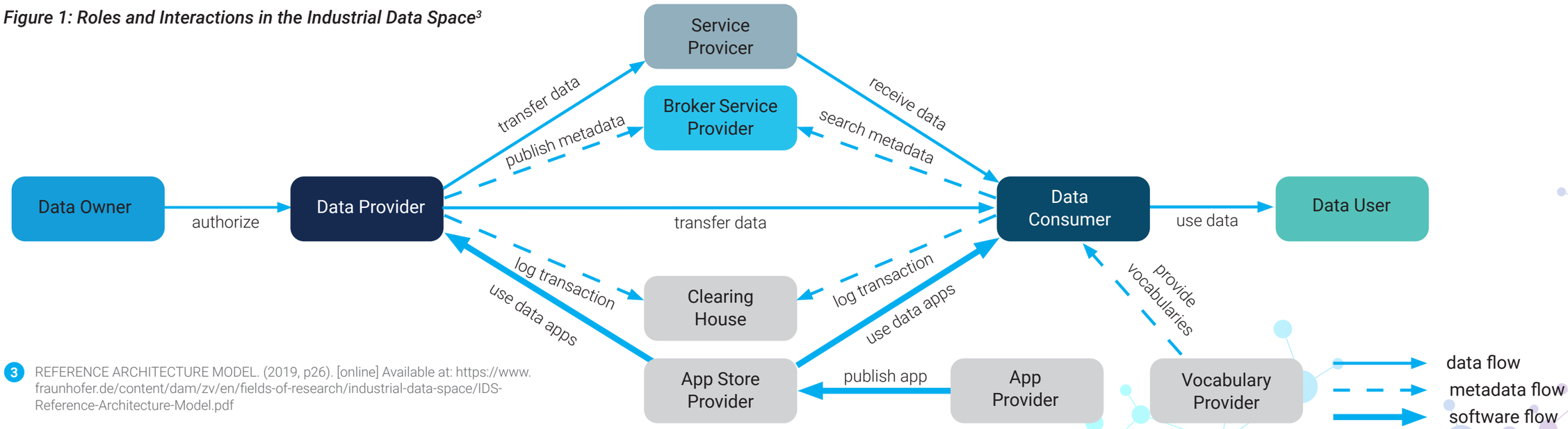
- Data Owner
- Data Provider
- Broker Service Provider
- Data Consumer
- Data User

Overarching governance of the IDS is provisioned through another key role - Certification Bodies.

One of the key advantages of the IDS model is its flexibility. The Data Owner can choose whether or not to share their data via a cloud platform or by peer-to-peer arrangement through the Broker Service Provider. Through the use of meta-data, the Data Owner can even describe those parts of individual data sets that may have restricted (or non-restricted) access rights by the Data Consumer and licensed usage rights by the end Data User.

This is a very simplified description of some of the roles. There are others which play important parts in the exchange and use of the data (e.g. App Stores) and we recommend a thorough reading of the IDS Reference Architecture Model Version 3.0 paper to understand their contribution to the process. We should emphasise that the Data Owner still owns the data even if it is processed outside of their immediate environment by a licensee (Data User). The model allows the Owner to set the parameters on usage and expiration – or in other words, 'cloud based' permanent access permissions on the data.

*Figure 1: Roles and Interactions in the Industrial Data Space*[3]




3 REFERENCE ARCHITECTURE MODEL. (2019, p26). [online] Available at: https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/IDS-Reference-Architecture-Model.pdf

# Cloud and new business models

How can cloud technology facilitate secure data exchange and how can a reference model like the IDS apply rigour to the process of data transaction?

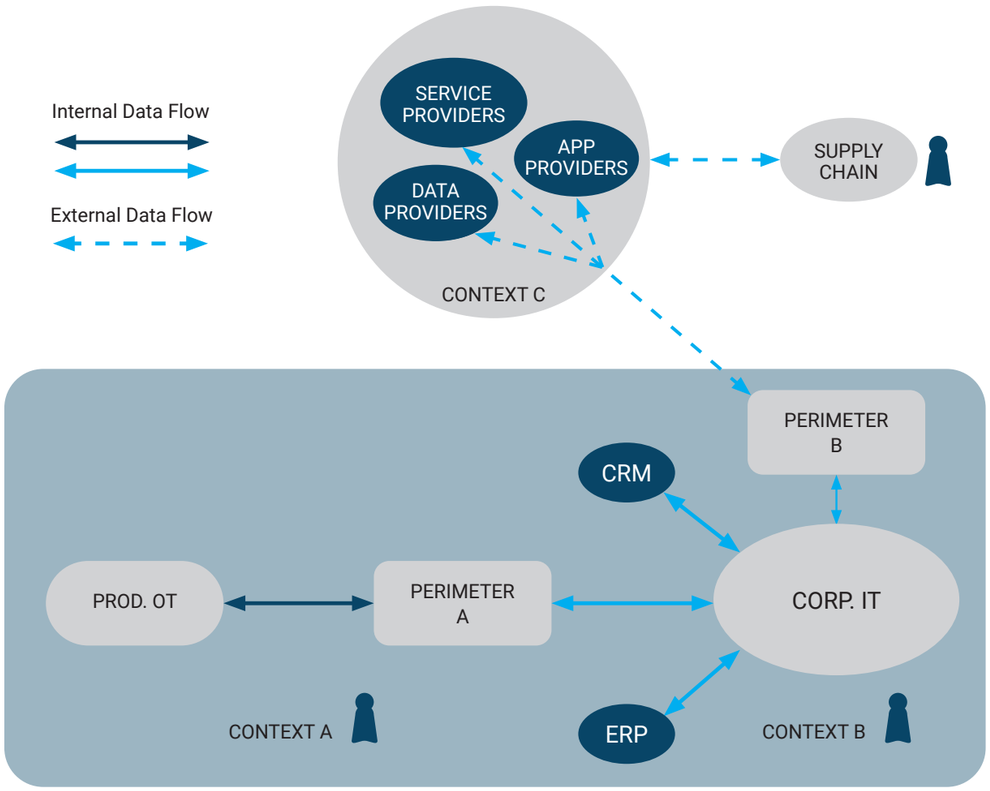



*Figure 2: Traditional Industrial & Enterprise Interactions*



Cloud based solutions are increasingly permeating business environments. Software as a Service, the practice of accessing software over the internet via a third-party provider, is already commonplace with the industry worth an estimated $141 billion in 2019[4]. The industry has seen exponential growth over the past decade, demonstrating the willingness of businesses to outsource their software needs where a suitable service is available. A third-party cloud service provider which collects and stores OT data, allowing for easy access and analysis in real time, could easily see a great deal of demand from businesses which struggle to make this process run smoothly internally. What needs to be considered is how third parties can obtain that data and do so in a secure manner.

In theory the best way of keeping OT systems secure, is to keep them isolated. (as in Figure 2 above) If they exist solely on their own networks, then they can't be interfered with. However, in practice most OT systems are already connected to the internet for a variety of reasons, meaning that additional security levels are required. A common example is the provision of 3rd party access to equipment by a maintenance company to gather operation statistics, such as the level of vibration on a turbine[5]. These systems use OT specific firewalls or modems for security, which allow only specific protocols to connect. Their best defence, however, is often 'security by obscurity', whereby they avoid being targeted in attacks as potential attackers are simply unaware that these connections exist. However, these connections, under controlled conditions, mean that the potential to export data outside of the network, thus to the cloud, already exists!

How does this happen? Traditionally, most ICS networks are siloed into different process areas, each managed, maintained, controlled and potentially operated by different suppliers who may utilise different security systems. It can get complicated and expensive very, very, quickly...

4 https://www.statista.com/statistics/510333/worldwide-public-cloud-software-as-a-service/

5 An example of NCSC Anti-Pattern for browse down, a story for another day!

Perhaps a better approach might be to move the perimeter (or DMZ) between production and corporate networks to Cloud based systems (see Figure 3 below), where the appropriate OT and Cloud controls and cyber-security operations could be centralised and managed at each of the following stages:

> Secure Acquisition (getting the right data, and preventing all other data from being exported)

> Secure Data Transport (between OT and Cloud)

> Secure Analytics (manufacturer accessing data for processing / analysis – maintaining sovereignty is crucial here)

This means that the security needs of the business (or Data Owner) can be met and scale across a range of platform providers, who can contribute services that play a part in the lifecycle of the data that is being produced by physical assets. This makes a lot of sense because the level of security investment by a Cloud provider will always exceed that of an individual organisation. It also promotes shared responsibility for the data asset across the internal and external stakeholders of the organisation as well as scaling according to need.

Once the OT data is in the Cloud, IT systems would then connect to the cloud through the usual methods, enabling them to access the data on demand and alleviating the need for complex OT/IT interconnectivity across multiple sites and zones.

In simple terms then, the perimeter of the ICS network should be moved to the Cloud for all the sites within the organisation. Why? It only needs to be built *once*.

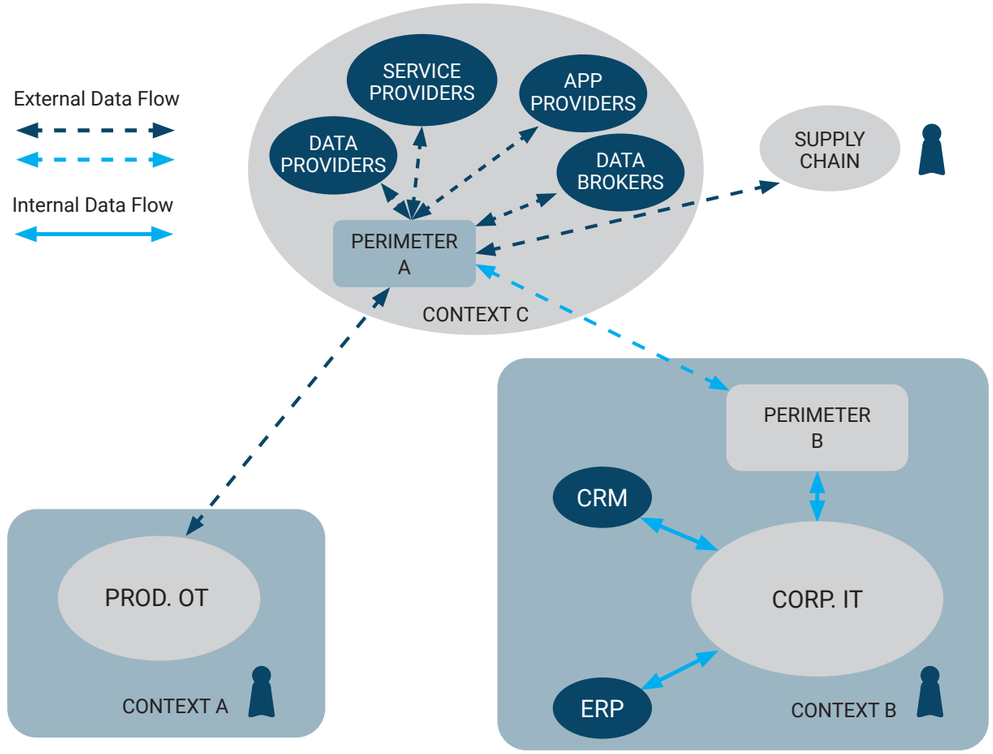



***Figure 3: Industial Data Space Architecture & Enterprise Interactions***

# The potential

Currently, on-premise OT systems are extremely proprietary in nature, with little to no compatibility between different manufacturers depending on the industry in which they are deployed.

The same approach is also being adopted on Cloud platforms as industrial vendors begin to transition their products and services to them. An example of this is GE's Predix which offers a cloud-based connection between different systems but is not directly compatible with other such Cloud based services such as Siemen's MindSphere or Cisco Kinetic.

Using the IDS reference architecture would allow for standardised approaches towards data sharing, enabling access to data created by machines from different manufacturers. Businesses will see a return on investment in the architecture not only through integrating with the supply chain, but also by the early catching of potential machine issues, enabling just-in-time production and cloud factories providing statistics on which parts are needed. In this manner, competition can be introduced into the supply chain. If a preferred supplier has problems, then through the use of Data Brokers a business can easily advertise its needs to other potential suppliers.

It's worth reminding ourselves that security relations between OT and IT are 'difficult' at best and incompatible at worst. However, cloud based data services such as those described in the IDS Reference Model will allow that OT data to be securely transferred, stored and then accessed by IT systems utilising standard security measures.

Scalability can be facilitated through the Managed Service Provision of a secured perimeter in the Cloud, resulting in almost unlimited growth potential. The ability to create more data consumers, including data (end) users and new customers throughout the supply chain is a real benefit – rather than a cost to the business.



# ABOUT POLESTAR

Polestar is an Industrial IoT company based in Nottingham, UK delivering services across Europe, Asia and North America. We have been providing secure & highly available infrastructure through our consultancy, design, delivery and support services since March 1998.

Polestar's core product is our consultative approach combined with our specialist knowledge. Our expertise in 'connected platforms' gives us the ability to deliver our services in the following 3 key areas of Industrial IoT:

- Data Acquisition
- Data Transport
- Data Analysis

We have extensive experience in maximising our clients' return on investment in OT / IT while helping them to create and maintain their competitive advantage. Our purpose is to share innovative, cutting edge technology and our expertise to other businesses and organisations.

We achieve this by putting the right people at your disposal, working with the very best partners in the industry and by refusing to compromise on data integrity or core business activities, placing continuity and high availability at the heart of our solutions.

For more information, visit www.polestarinteractive.com.

# ABOUT NEXOR

Nexor is a secure information exchange specialist with an extensive track record of successfully delivering cyber security solutions to defence and critical infrastructure organisations around the globe, including the UK MOD, GCHQ, Transport for London, the Metropolitan Police Service, Europol and NATO.

Nexor's roots in developing innovative technology solutions were established in the late 1980s when the business was spun out of a communications research programme at the University of Nottingham and University College, London. Our technology brought a new paradigm in functionality and interoperability to open systems messaging.

From this foundation in high grade security applications, we have focused our capability on secure information exchange and cross domain applications within government, defence and critical national infrastructure sectors. As of today, several hundred guards and gateways based on our technology have been deployed throughout the allied defence and security community.

Today our typical customer needs protection from advanced threat actors that may specifically target their organisation using bespoke techniques to gain access to valuable information assets or attempt to control systems. Nexor utilises its extensive experience in this realm to develop sovereign high assurance information exchange solutions that enable cross domain interoperability and interworking following NCSC (the UK's National Technical Authority) guidance.

Nexor's products are designed and delivered in accordance with Nexor's Secure Information eXchange Architecture (SIXA®) and our services are underpinned by our CyberShield Secure® agile methodology. Together these ensure objectives are defined and that successful outcomes are measurable, whilst keeping a business's digital transformation objectives at the heart of any solutions we implement. This is further supported by our formal certifications which include TickITplus, ISO9001, ISO27001 and Cyber Essentials Plus.



# ABOUT THE AUTHORS

**JULIAN SMITH**

Julian Smith is Managing Director of Polestar Interactive and a Chartered Manager. After graduating from Nottingham Trent University, Julian joined Polestar and trained as a Cyber Security Engineer. He has worked extensively with global brands including Carlsberg, Delta Airlines, Jaguar Land Rover, UDG and many others.

**COLIN ROBBINS**

Colin Robbins is Managing Security Consultant at Nexor where he leads the team delivering CyberShield Secure® services. He is a Fellow of the Chartered Institute for Information Security and a NCSC Certified Professional. Colin has provided his expertise across the defence, police and energy sectors.

For more information about any of the information provided in this document please contact Polestar or Nexor

+44 (0)115 911 6699
www.polestarinteractive.com
info@polestarinteractive.com
The Sir Colin Campbell Building, University of Nottingham Innovation Park, Triumph Road, Nottingham, NG7 2TU, UK

+44 (0)115 952 0500
www.nexor.com
info@nexor.com
8 The Triangle, Enterprise Way, ng2 Business Park, Nottingham, NG2 1AE, UK