

Dataflow Challenges in an *Internet of Production*

A Security & Privacy Perspective

Jan Pennekamp, Martin Henze, Simo Schmidt, Philipp Niemietz, Marcel Fey, Daniel Trauth, Thomas Bergs, Christian Brecher, and Klaus Wehrle

INTERNET OF PRODUCTION | RWTH AACHEN UNIVERSITY

<https://comsys.rwth-aachen.de/>

London / ACM CPS-SPC 2019, 11th November 2019

Vision of an Internet of Production (IoP)

- **Federal-funded research cluster in Aachen, Germany**

- ▶ Over 35 institutes in Aachen, ~ 50 Mio € in funding



- **Goal is to create a “World Wide Lab”**

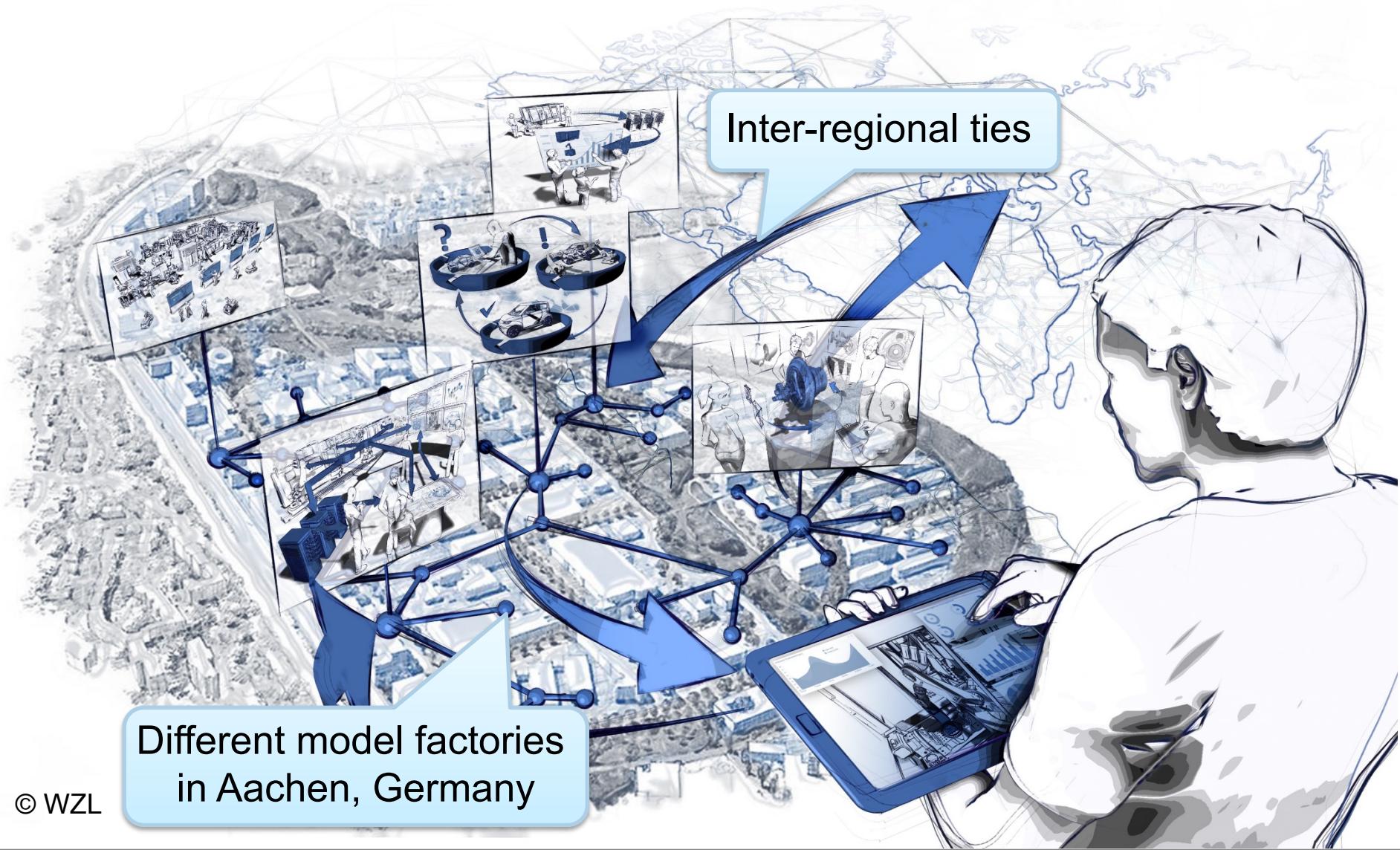
- ▶ To *utilize data* from production, development and usage
- ▶ In real time (adaptively) with an adequate level of granularity
- ▶ Even in *cross-domain collaboration*

- **Establishing a Google-like engine for production queries**

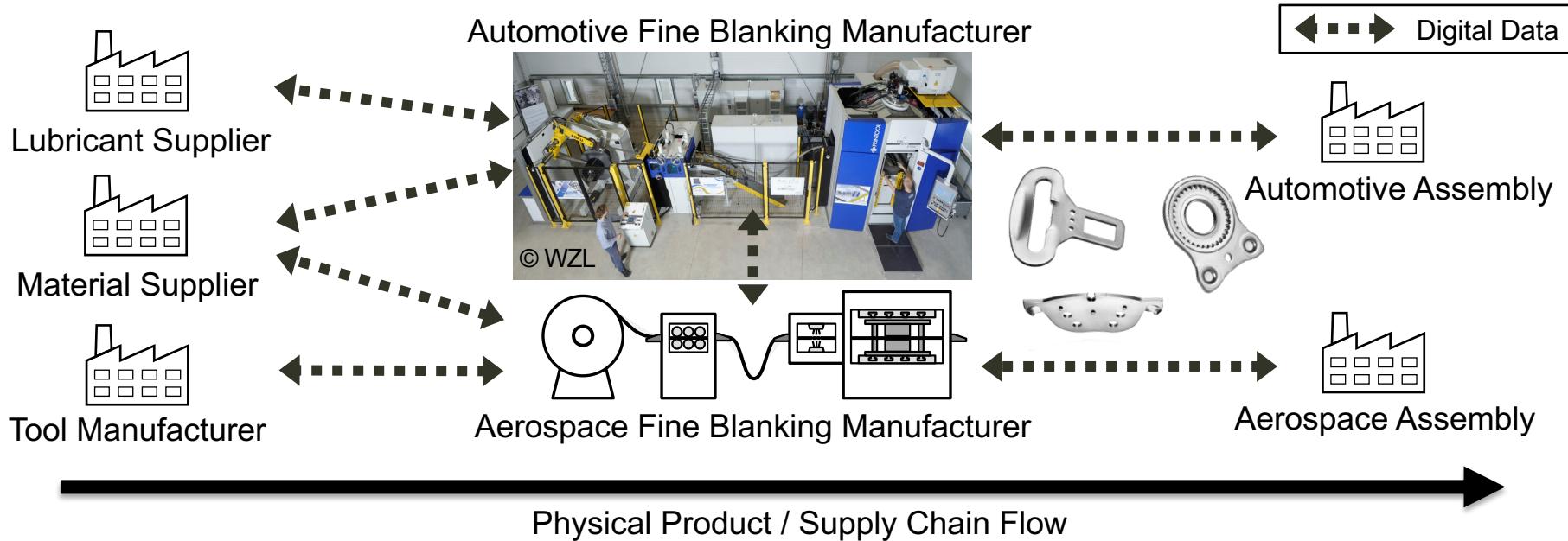
- ▶ Merging models and massive data to optimize processes



Illustration of an Internet of Production (IoP)



Use Case: Collaboration of Fine Blanking Manufacturers



- **Fine Blanking Line**

- ▶ Integrating external information along the supply chain
 - ▶ Manufacturers can exchange information of their CPS, the processed material and their interplay

Issues with accountability?

Leakage of process information?

A Case for Integrated Data Processing in Large-Scale Cyber-Physical Systems

René Globus¹, Martin Heuer², Philipp Nimmerl³, Daniel Tausch⁴, Patrick Matfäß⁵, Thomas Berg³
¹Technische Universität Darmstadt, ²WZL Institute for Machine Tools and Production Engineering, ³WZL Institute for Machine Tools and Production Engineering, University of Würzburg, ⁴WZL Institute for Machine Tools and Production Engineering, University of Würzburg, ⁵WZL Institute for Machine Tools and Production Engineering, University of Würzburg

Abstract

Large-scale cyber-physical systems such as manufacturing plants or cities require a large amount of data to precisely control their machines. Making such data available to all stakeholders in real time is a challenge. In this paper, we show how this data available also to computation systems outside the factory floor can be used to improve the system. We show, among amounts and completeness of data and communication requirements, how to reduce transmission, storage, and processing to its limits. In this paper, we propose a new approach that takes into account the need to process up to 6.2 million events per day to obfuscate the data requirements found in modern manufacturing.

Manufacturing processes are highly dynamic and data processing which keeps latency and bandwidth low is required. In this paper, we propose a novel time centralized data relay using more complex distributed processing. This approach allows for both maintaining control of individual parts and decreasing the benefits of “big data” applications.

1. Introduction

Modern manufacturing data usually generates orders of magnitude more data than actual products. Cyber-physical systems (CPS) have the potential to turn this data into a valuable resource for decision making, to support the Internet of Production [2]. Increasingly digitized manufacturing systems are able to collect data from various sources, including suppliers, manufacturers, and customers. This enables highly integrated value chains that couple the design and development aspects of the production process, yielding increased product quality [3] and more efficient manufacturing environments [4].

One distinct characteristic of cyber-physical systems is the need to process data in real time. Due to their ability to utilize real-time data collected during manufacturing processes, data processing is a core process [5], potentially integrated into large-scale systems for supply chain management. Real-time data processing is a key feature of manufacturing processes makes it easier to detect and react to sudden changes in the environment, such as variations in working conditions or equipment failures, consequently increasing the efficiency of the system. This also enables unprecedented traceability of goods. Individual components of a CPS can be tracked throughout the manufacturing of individual parts or products [6], enabling traceability of the entire product life cycle and quality in case of fluctuations in quality.

Due to the high volume of data generated by manufacturing systems, continuous to increase, more efficient data processing is required for capturing, storing, and processing this data [7]. Eventually, data processing will become a bottleneck in CPS. Likewise, processing and storage capacities close to the data source are required to keep latency low. Offloading, offering efficient to input signals down to the edge of the network, is a promising way to reduce latency or adapting to the data rates. In contrast, off-line computing and storage [8] can only work with static data and therefore do not support fast and unpredictable latencies and transient load, just as the data is being processed.

In this paper, we focus on the potential of distributed processing in large-scale CPS. The proposed system is able to cope with the latency and bandwidth requirements of distributed processing. The proposed an integrated and adaptive approach which takes into account the amounts and completeness of the respective tasks. Local and distributed processing are combined to handle more complex decision processes can be handled in near-optimal centralized. Consequently, we propose methods to select appropriate data

Use Case: Benefits for Connected Job Shops

- **Connected Job Shop**

- ▶ Identify root causes of failure more easily (more available data)
 - ▶ Reduce scrap due to an improved process ramp-up time
 - ▶ Manufacturing-as-a-Service

Access to external data



Access to the local process



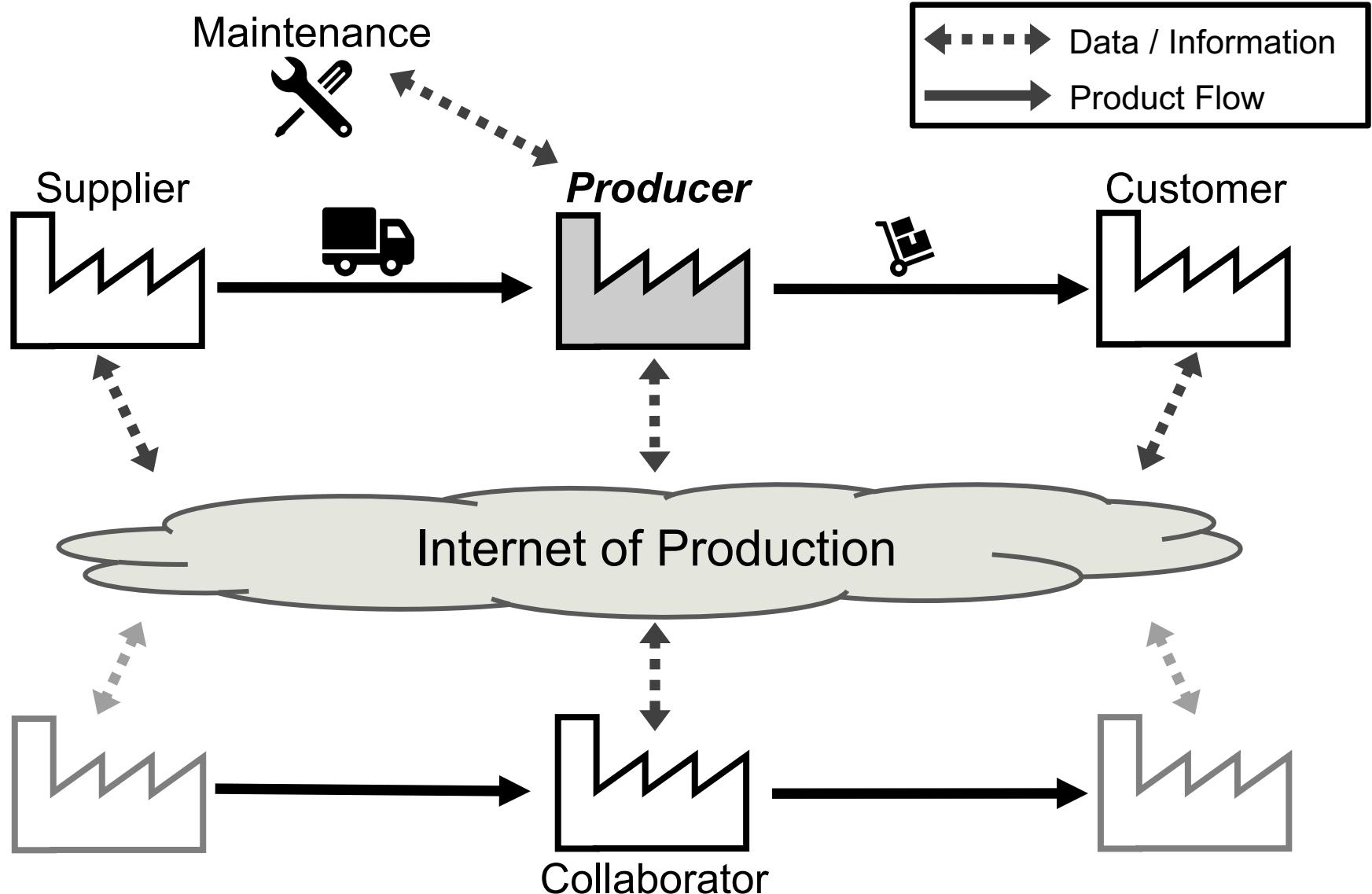
© WZL



Realistic laboratories with interconnected machines

Dataflow Challenges in an Internet of Production: A Security & Privacy Perspective

Overview of Actors



Overview on Entities



Producer

- Our central point of view
- Can also be a supplier, collaborator, or customer
- Reports to / interacts with other entities in the landscape



Supplier / Customer

- Delivers / Receives materials or (intermediate) products along the supply chain
- Existing business contracts
- Last recipient is end customer



Maintenance

- Directly interacts with entities to fulfill service contracts
- Usually access to the machines, tools, and their (usage) data



Collaborator

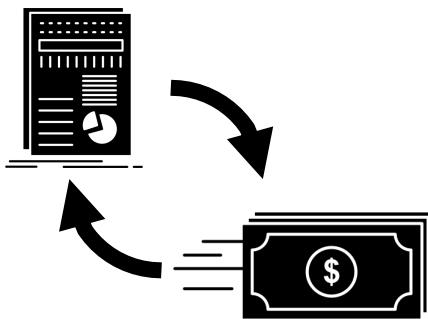
- Part of another supply chain
- Participating in inter-organizational dataflows
- Comparable / related process as considered producer

Advantages for Collaborators along the Supply Chain

-  **Supplier &  Producer**

- ▶ Machine supplier has direct access to usage information
 - Threat of (process) reverse-engineering
- ▶ New concepts: Manufacturing-as-a-Service, Pay-per-Part
- ▶ Usage values can shape the supplied parts/machines/tools

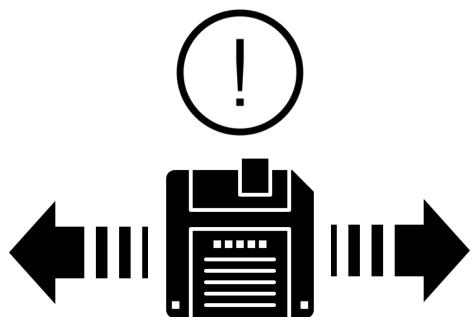
-  **Producer &  (End) Customer**



- ▶ Comparable relationship (different viewpoint)
- ▶ Information can be traded for discounts
 - Sensitive data can help to adjust the process
- ▶ Usage data can help to improve the customer's satisfaction (e.g., updates)

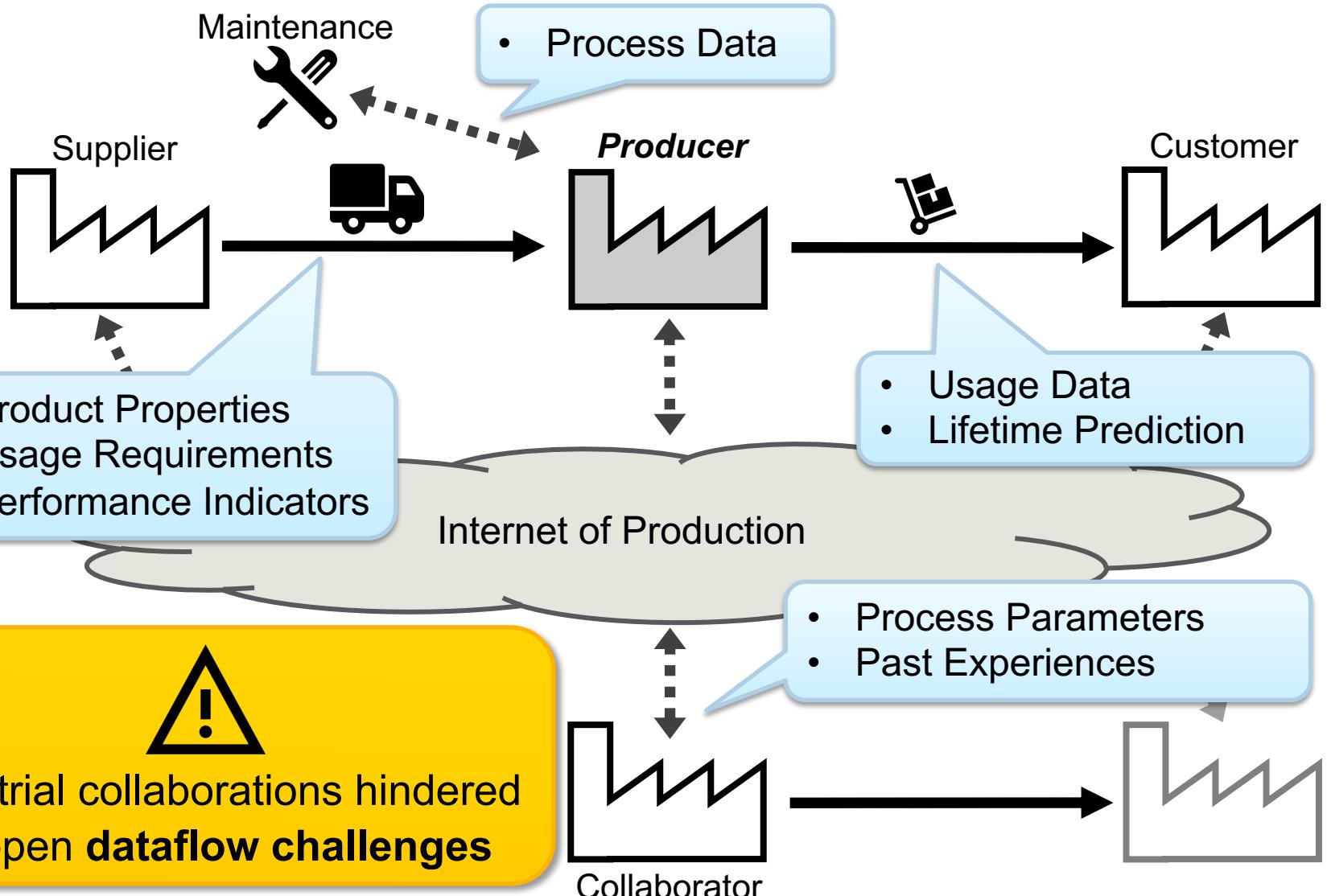
-  **Maintenance &  Producer**

- ▶ Insight into the process to provide best possible service
 - Knowledge might transfer unintentionally to competitors
- ▶ Maintenance provider might be responsible for (firmware) updates
 - Risk of malicious (external) code



-  **Producer &  Collaborator**
- ▶ Inter-organizational dataflows promise advances
 - Improve productivity & decrease process setup
 - ▶ Flexible relationships to retrieve knowledge
 - Caution, especially, with anonymous collaborators

Dataflows Contain Information Worth Protecting



Missing Parts to Address Open Dataflow Challenges

Authenticity of Information

- Aspects related to *correctness* & *origin* of data
- Companies require utilized data to be *reliable*
- Provides means to enable *accountability* & liability



Industrial setting shows strong requirements for correctness

Scope of Data Access

- Implementing *confidentiality* and limiting data *granularity*
- Authentication & authorization for *control over data*
- Concerns regarding unauthorized data forwarding



Privacy needs of participants must be upheld at all times

Anonymity

- Pseudonyms can help to protect the identity of companies
- Actions within an IoP should be *untrackable*
- Counter the aversion of sharing data in today's companies

Surveyed Security & Privacy Building Blocks

Data Security

- Target confidentiality
- Distribute data control

Data Processing

- Tackle the scope of data access
- Secure computations or secure offloading

Platform Capabilities

- Establish infrastructure-supported concepts

Proving Support

- Implement verifiability and logging
- Linking between digital and physical object

External Measures

- Enable new approaches (e.g., data markets)
- Create legal framework

How to **address** the open challenges with these building blocks?

Overview Table of Surveyed Building Blocks

	authenticity	integrity	accountability	auditing	immutability & referenceability	confidentiality	granularity	authentication	authorization	data control	identifiability	untrackability
	Authenticity of Information				Scope of Data Access				Anonymity			
Data Security												
Encryption [7]					++				+			
Data Usage Control [52]		+		+	++	+		+	+	++	+	+
Secret Sharing [60]	+		+		+				++		+	+
Data Processing												
Secure Offloading [10]					++				+		++	+
Secure Computation [43]					++				++		+	+
Anonymization [62]					+	++					+	+
Proving Support												
Digital Fingerprints [71]	++				++			+				--
Digital Signatures [55]		++			++	+						--
Distributed Ledgers [44]	++		++		++	++						+/-
Version Control [40]		+			+	++		++				+
Platform Capabilities												
Access Control [57]					+				++			
Policies [32]					+				++			
Smart Contracts [75]	+	+	++		+				+			
Trusted Computing [58]	++	++	+		+			+	+			
External Measures												
Data Markets [5]					+				++			
Legal Contracts [4]					-	++		++				
Smart Payments [34]									+			

Digital fingerprints help to track components precisely

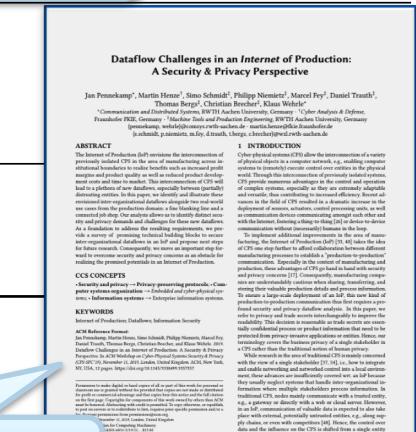
Compute on sensitive data with collaborators

Data markets can ease exchanges with competitors

- Applicability rated in the range of ++ to -

► When measurable

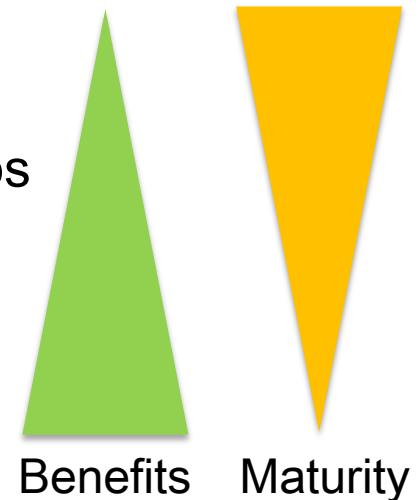
For details, check the paper



1. Stakeholders must communicate their individual needs

2. Implementing the Internet of Production

- i. Improving existing (industrial) business relationships
- ii. Integrating data of non-competitors
- iii. Utilizing process data of (direct) competitors

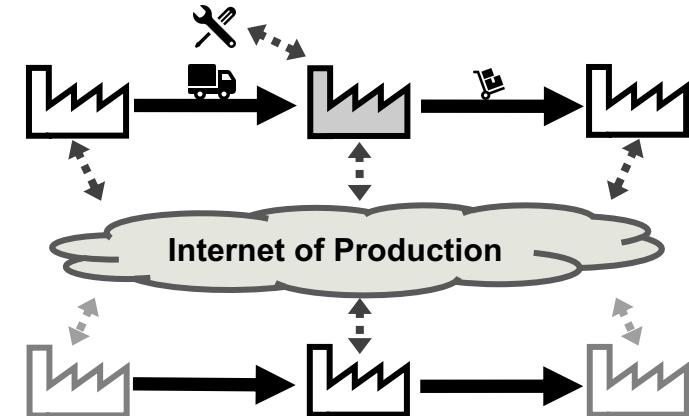


Experiences gathered in one stage help to shape data **security and privacy** in subsequent stages

Conclusion: Strong Need for Security & Privacy

- **Different needs for industrial collaborations exist**

- ▶ Five entities 
- ▶ Analysis based on real-world use cases
 - Fine blanking line
 - Connected job shop
- ▶ Realized benefits depend on improved security & privacy approaches



- **Presented three main categories of challenges**

Authenticity of Information

Scope of Data Access

Anonymity

- **Various building blocks are relevant for future research**

- ▶ They can enable new ways of secure industrial collaboration
- ▶ No single one-fits-all solution exists