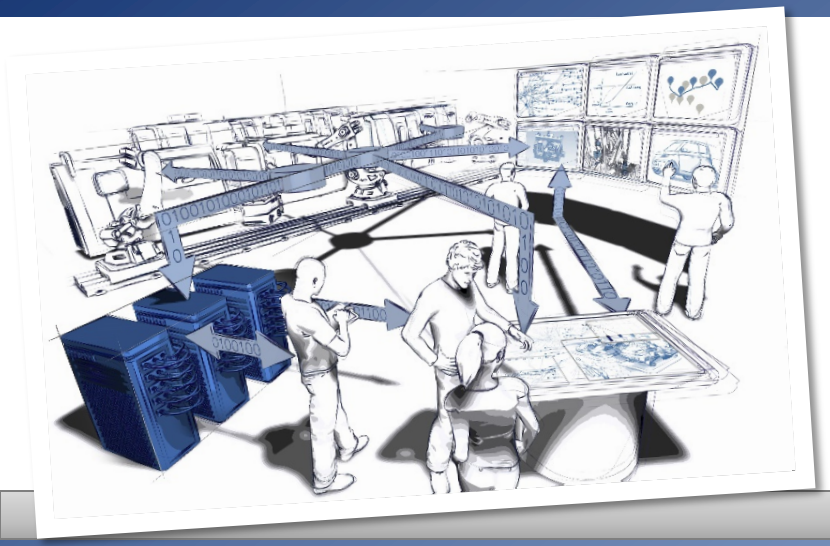


Dataflow Challenges in an *Internet* of Production

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

Fraunhofer FKIE | WZL | COMSYS | RWTH AACHEN UNIVERSITY

Vision of an Internet of Production (IoP)

- **Federal-funded research cluster in Aachen, Germany**
  - Over 35 institutes in Aachen, ~ 50 Mio € in funding

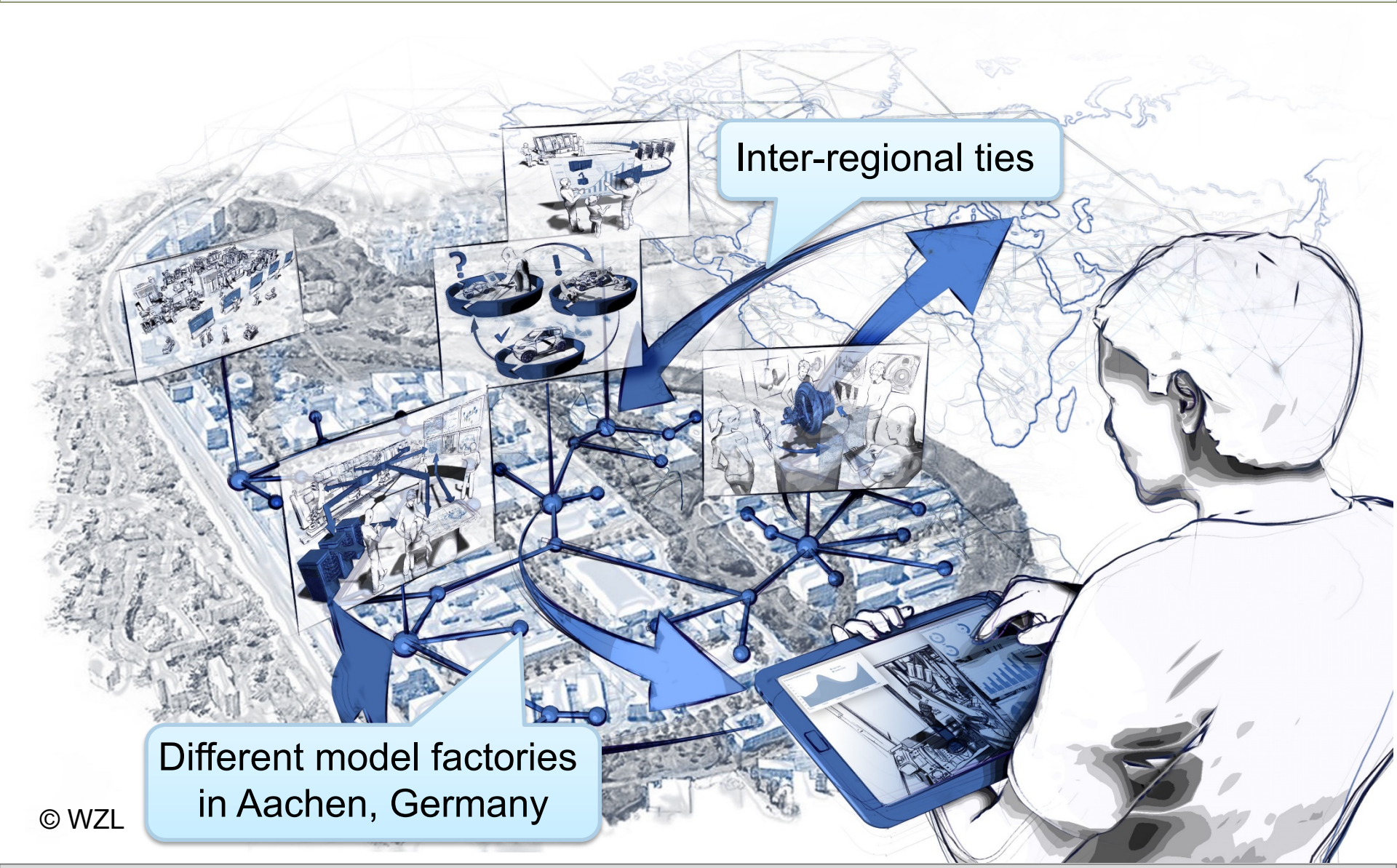
INTERNET OF PRODUCTION | RWTH AACHEN UNIVERSITY

- **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

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Illustration of an Internet of Production (IoP)

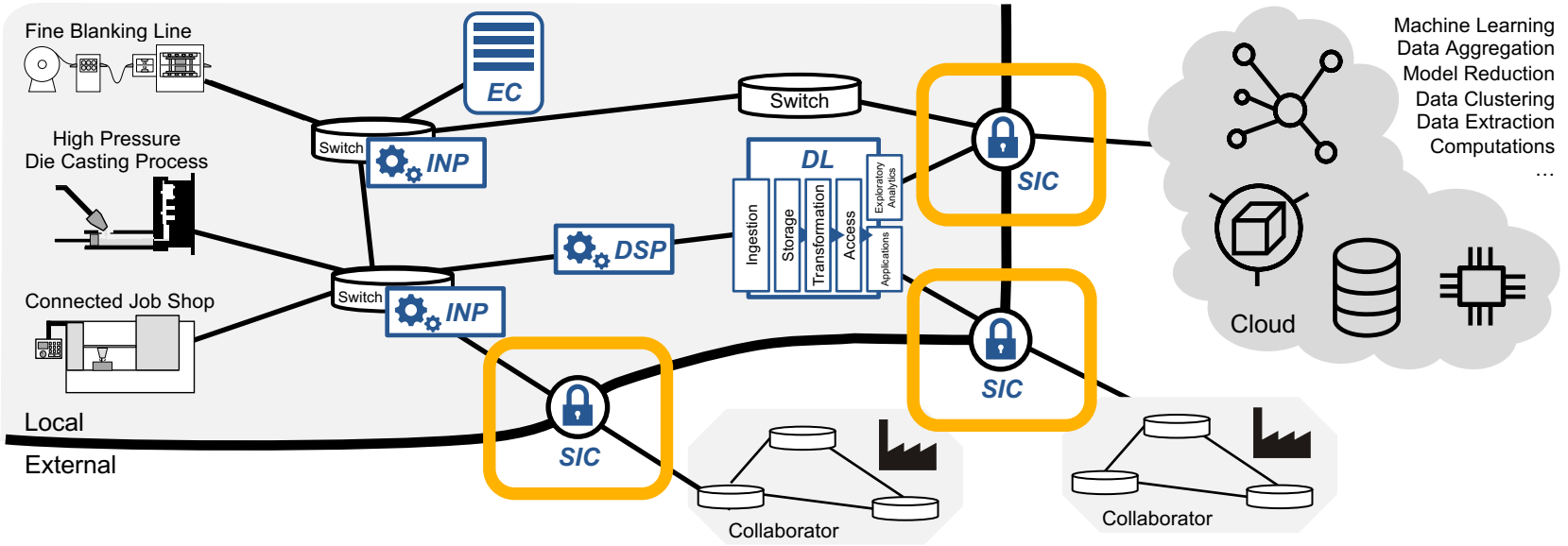


© WZL

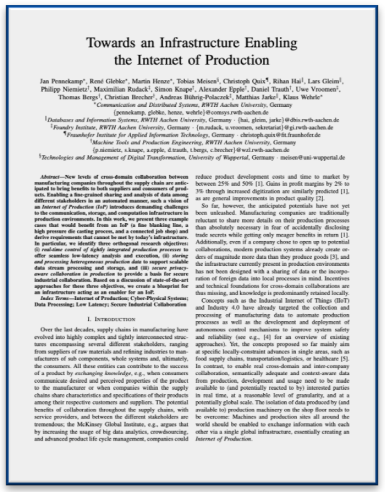
Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

A Brief Look at the Underlying Infrastructure

- **Crafting an infrastructure for the Industrial IoT**

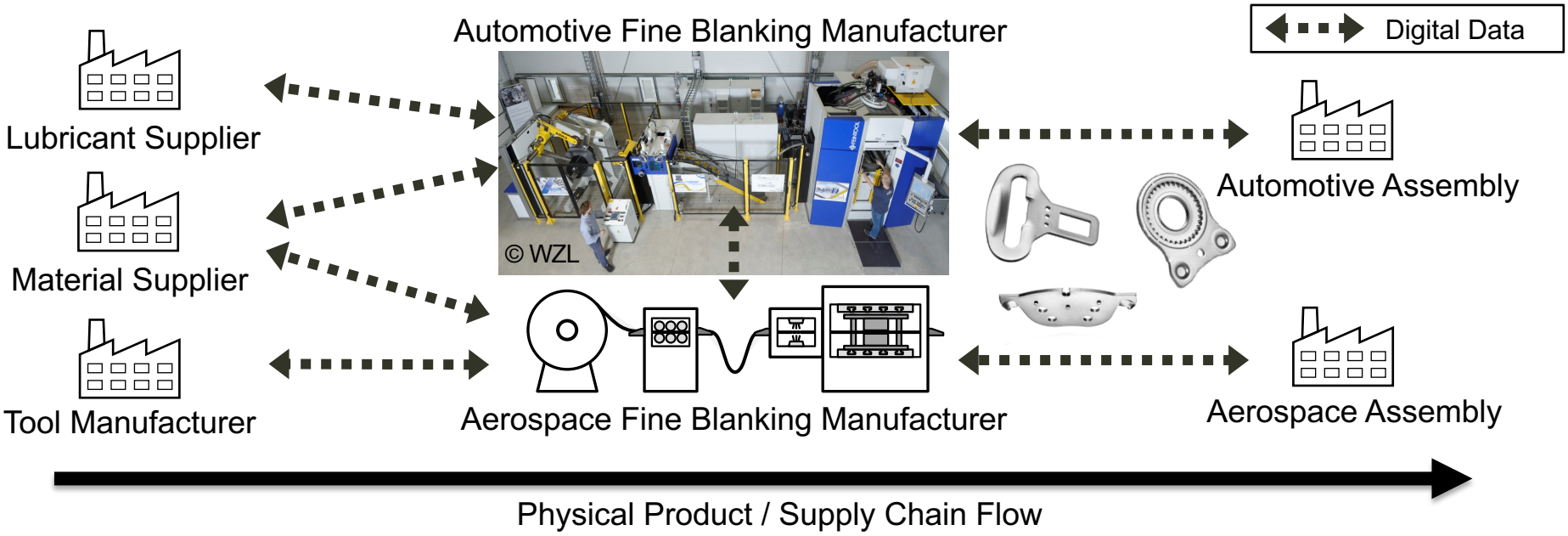


- **With three distinctive key concepts**
  - In-Network Processing (INP) & Edge Computing (EC)
  - Data Stream Processing (DSP) & Data Lakes (DL)
  - Secure Industrial Collaboration (SIC)


Towards an Infrastructure Enabling the Internet of Production

J. Pennekamp, R. Glebke, M. Henze, et al.: "Towards an Infrastructure Enabling the Internet of Production" @ *IEEE ICPS 2019*.

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

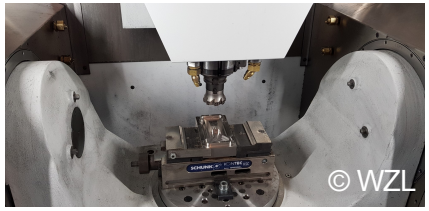
R. Glebke, M. Henze, et al.: "A Case for Integrated Data Processing in Large-Scale Cyber-Physical Systems" @ *HICSS 2019*.

COMSYS | RWTH AACHEN UNIVERSITY

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

Realistic laboratories with interconnected machines



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‡, Klaus Wehrle*

*Communication and Distributed Systems, RWTH Aachen University, Germany †Cyber Analytics & Defense, Fraunhofer FKIE, Germany ‡Machine Tools and Production Engineering, RWTH Aachen University, Germany

ABSTRACT

1 INTRODUCTION

CCS CONCEPTS

KEYWORDS

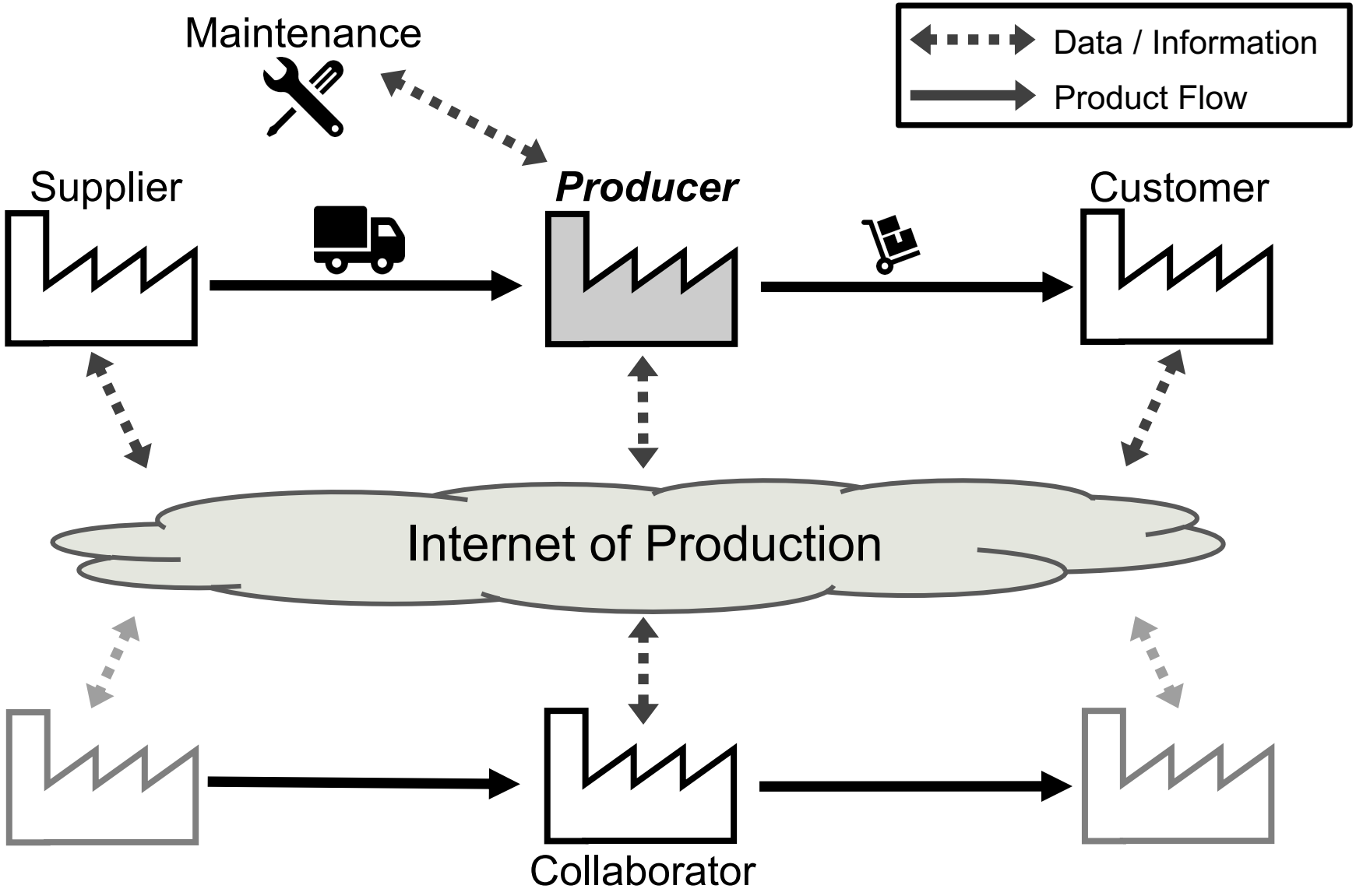
ACM Reference Format:

J. Pennekamp, M. Henze, et al.: "Dataflow Challenges in an *Internet* of Production: A Security & Privacy Perspective" @ *ACM CPS-SPC 2019*.

COMSYS

RWTH AACHEN UNIVERSITY

Overview of Actors



Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

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

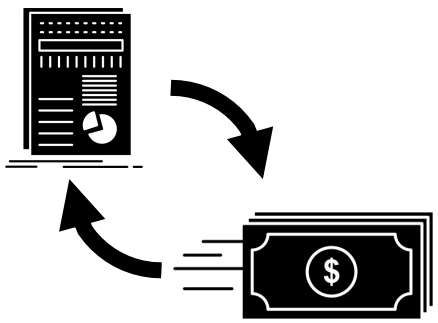
Collaborator

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

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

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

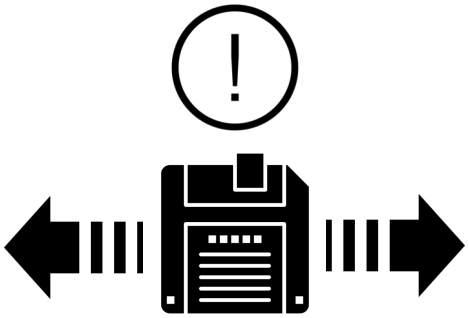


- **Producer & (End) Customer**
  - Comparable relationship (different viewpoint)
  - Information can be traded for discounts
    - Sensitive data can help to adjust the process
  - Usage data can help to improve the customer's satisfaction (e.g., updates)

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

IoP-supported Collaborations

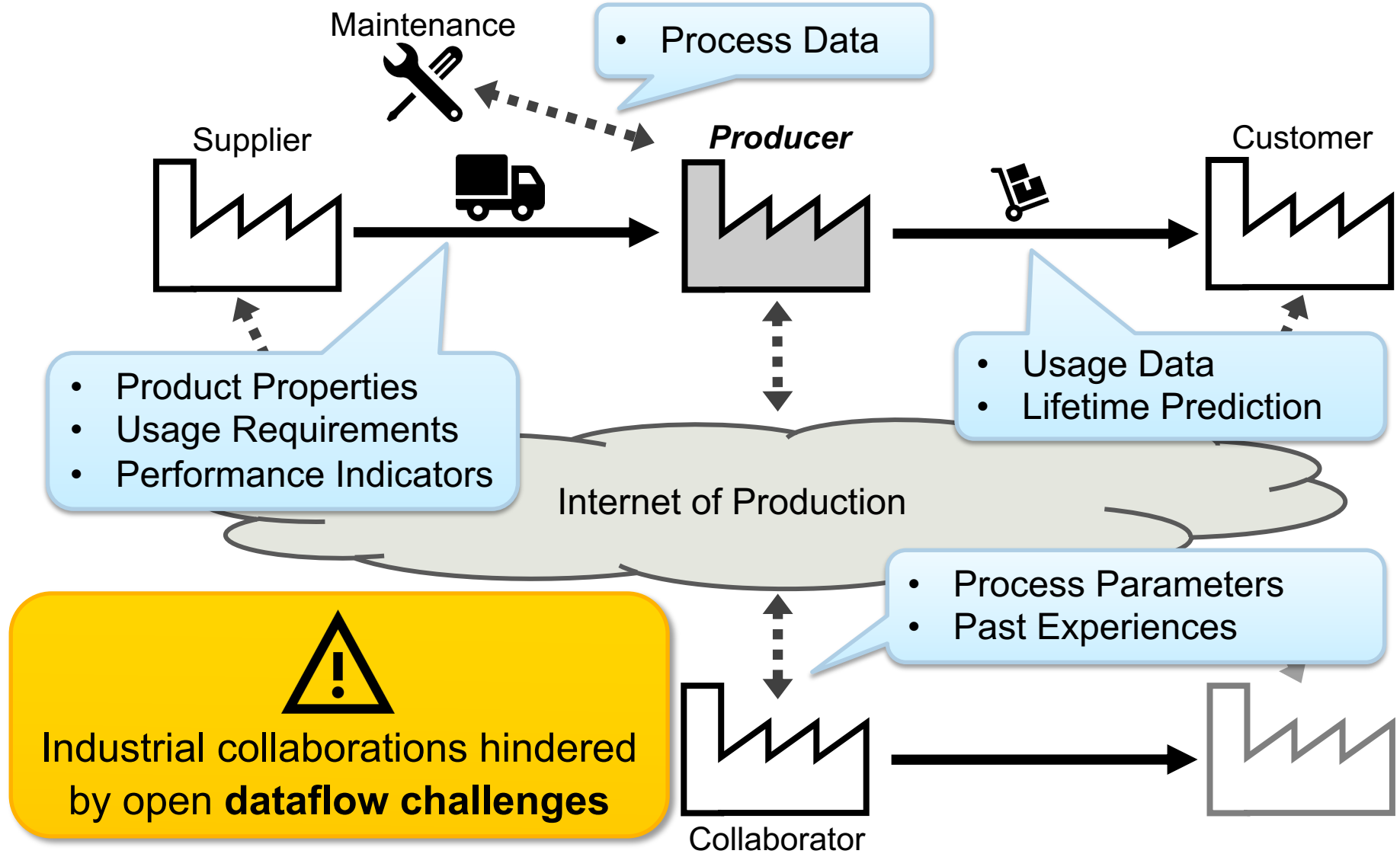
- **Maintenance & Producer**
  - Insight into the process to provide best possible service
    - Knowledge might transfer unintentionally to competitors
  - Maintenance provider might be responsible for (firmware) updates
    - Risk of malicious (external) code



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

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

Dataflows Contain Information Worth Protecting



Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

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

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

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

External Measures

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

Proving Support

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

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

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

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


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‡, Klaus Wehrle*

*Communication and Distributed Systems, RWTH Aachen University, Germany †Cyber Analysis & Defense, Fraunhofer FKIE, Germany ‡Machine Tools and Production Engineering, RWTH Aachen University, Germany

ABSTRACT

1 INTRODUCTION

CCS CONCEPTS

KEYWORDS

ACM Reference Format:

- **Applicability rated in the range of ++ to –**
  - When measurable

For details, check the paper

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

COMSYS RWTH AACHEN UNIVERSITY

Future Work: Next Steps in Realizing an IoP

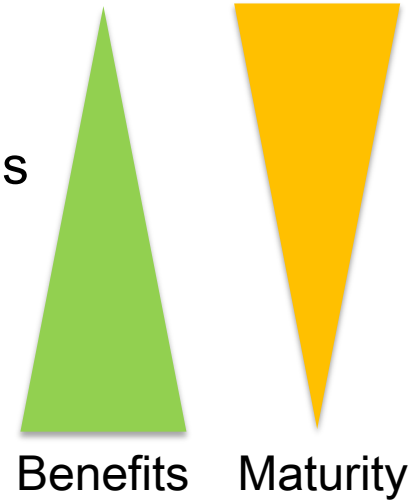
1. Stakeholders must communicate their individual needs

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

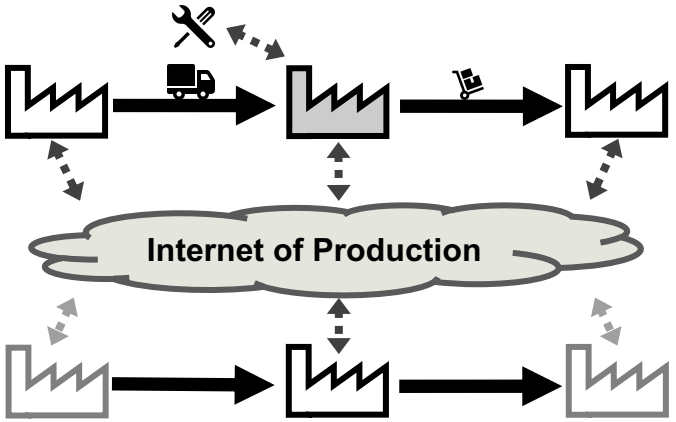


Experiences gathered in one stage help to shape data **security and privacy** in subsequent stages

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de

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

Jan Pennekamp
pennekamp@comsys.rwth-aachen.de