

# Trust 4.0: Dataflow-based Trust Modelling and Analysis in Industry 4.0 Systems

Spiros Alexakis (CAS Software AG), Stephan Seifermann (Karlsruhe Institute of Technology)  
Fachgruppentreffen GI Architekturen 2019

SOFTWARE DESIGN AND QUALITY GROUP  
INSTITUTE FOR PROGRAM STRUCTURES AND DATA ORGANIZATION, FACULTY OF INFORMATICS



TRUST4.0

# Trust in Industry 4.0



## Supply chains in Industry 4.0 are distributed and complex

- Many participants acting in various roles
- Many information exchanged between participants
- Information exchange vital for production



## Trust required between participants

- No confidential information must be shared
- Participants only allowed to see necessary information



## Situations might change rapidly

- Information sharing depending on geographical location
- Information sharing required by exceptional events



# Project Trust 4.0

## KIT

- Architectural Data Flow Modeling and Analysis



## CAS

- Requirements
- Privacy-aware decision making



## CUNI

- Runtime Access Control Modeling and Analysis



## IMA

- Requirements
- Privacy-aware sensor gateway



# TRUST4.0

Dataflow-based privacy for industry 4.0

Introduction



Running Example



Modeling and Analyses



Runtime Enforcement



Conclusion

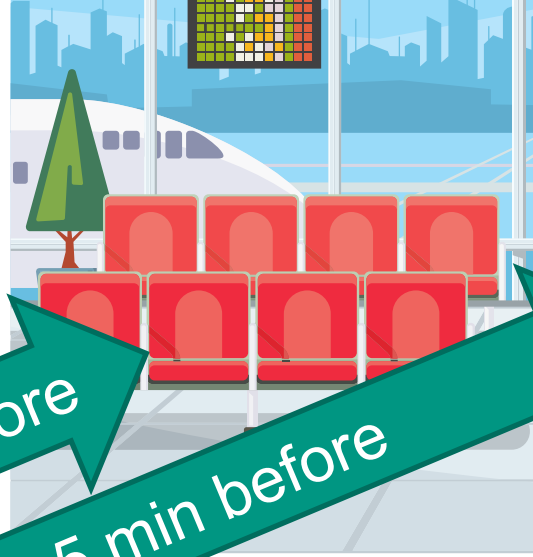
# Running Example

## Concepts

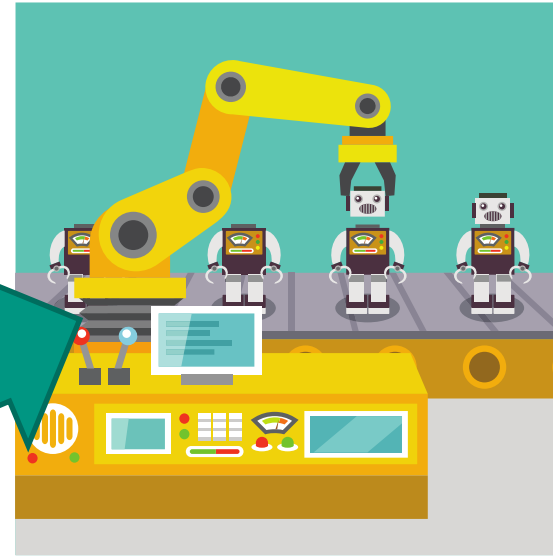
Employee's Homes



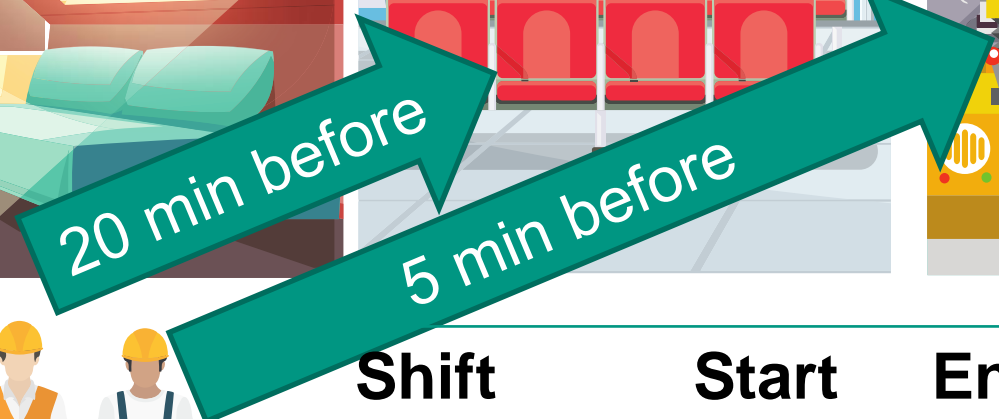
Factory Waiting Area



Factory Workplace



Factory Office



Shift	Start	End	Supervisor	Workers
PROD13	09:00	17:00	Susan	Werner Winfried

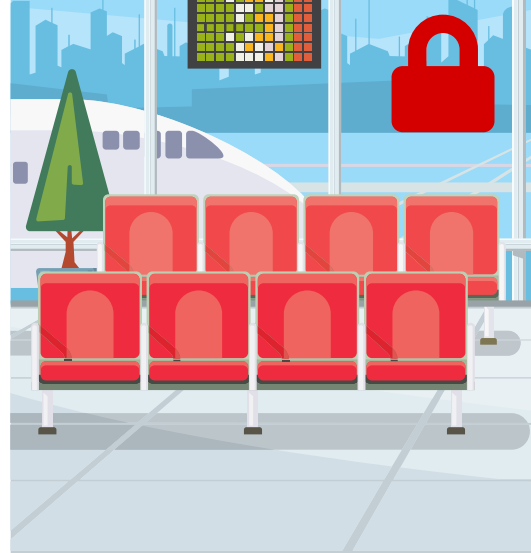


# Running Example Scenario

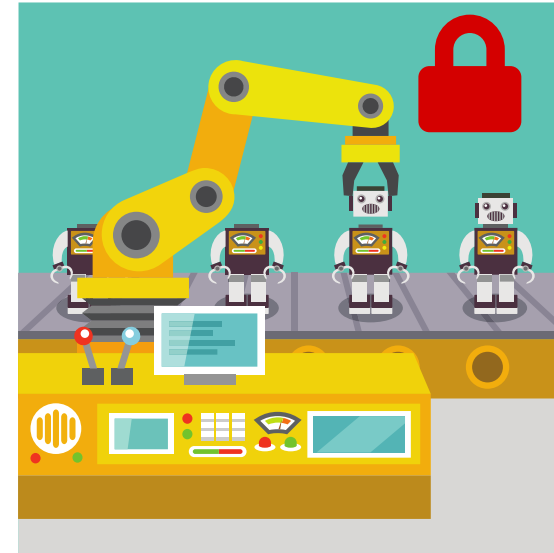
Employee's Homes



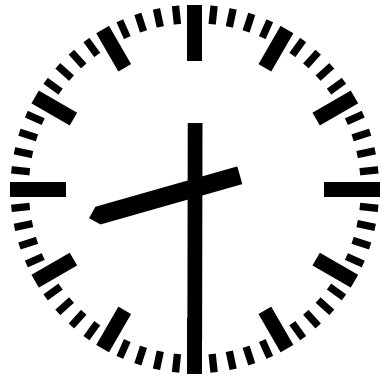
Factory Waiting Area



Factory Workplace



Factory Office



Shift	Start	End	Supervisor	Workers
PROD13	09:00	17:00	Susan	Werner Winfried



# Running Example Scenario

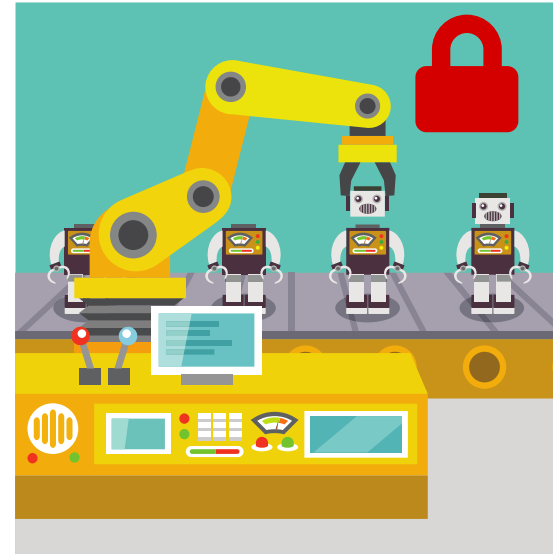
Employee's Homes



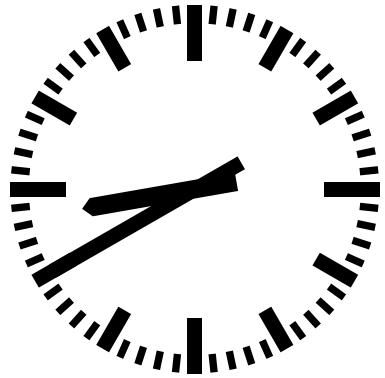
Factory Waiting Area



Factory Workplace



Factory Office



Shift	Start	End	Supervisor	Workers
PROD13	09:00	17:00	Susan	Werner Winfried



# Running Example Scenario

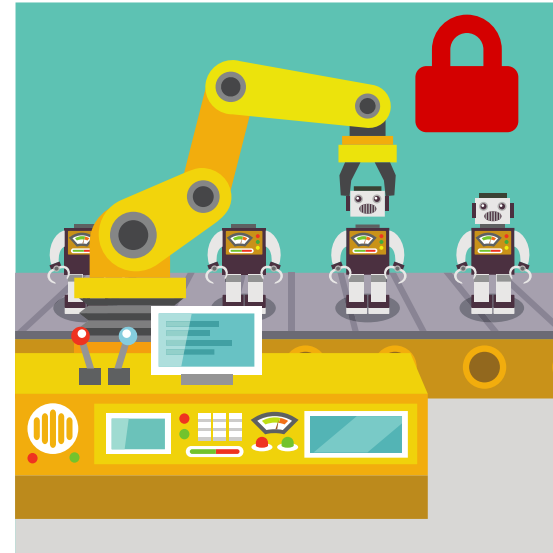
Employee's Homes



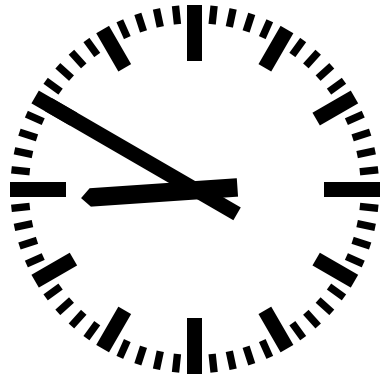
Factory Waiting Area



Factory Workplace



Factory Office



Shift	Start	End	Supervisor	Workers
PROD13	09:00	17:00	Susan	Werner Winfried



# Running Example Scenario

Employee's Homes



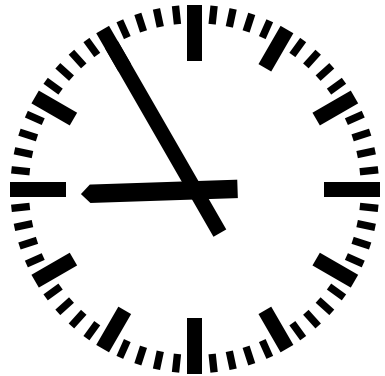
Factory Waiting Area



Factory Workplace



Factory Office



Shift	Start	End	Supervisor	Workers
PROD13	09:00	17:00	Susan	Werner Winfried



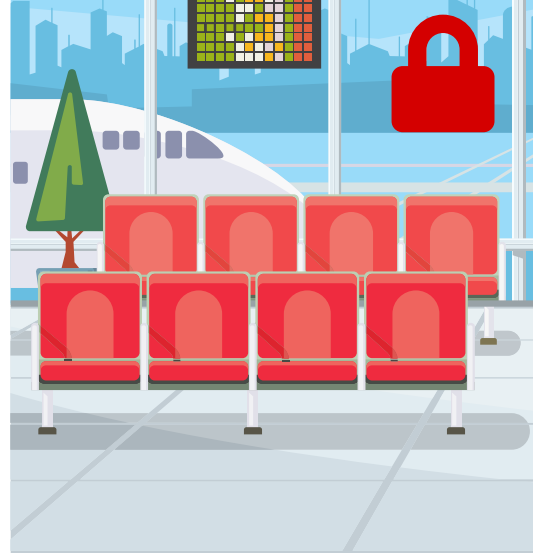


# Running Example Scenario

Employee's Homes



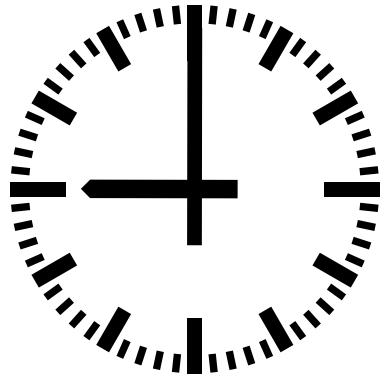
Factory Waiting Area



Factory Workplace



Factory Office



Shift	Start	End	Supervisor	Workers
PROD13	09:00	17:00	Susan	Werner Winfried



# Running Example

## Security Constraints

### Assets

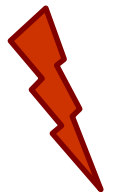
- Locations in factory
- Data about workers

### Physical Constraints

- Only workers assigned to shift can access factory 25 min before shift
- Only workers assigned to shift can access workplace 8 min before shift

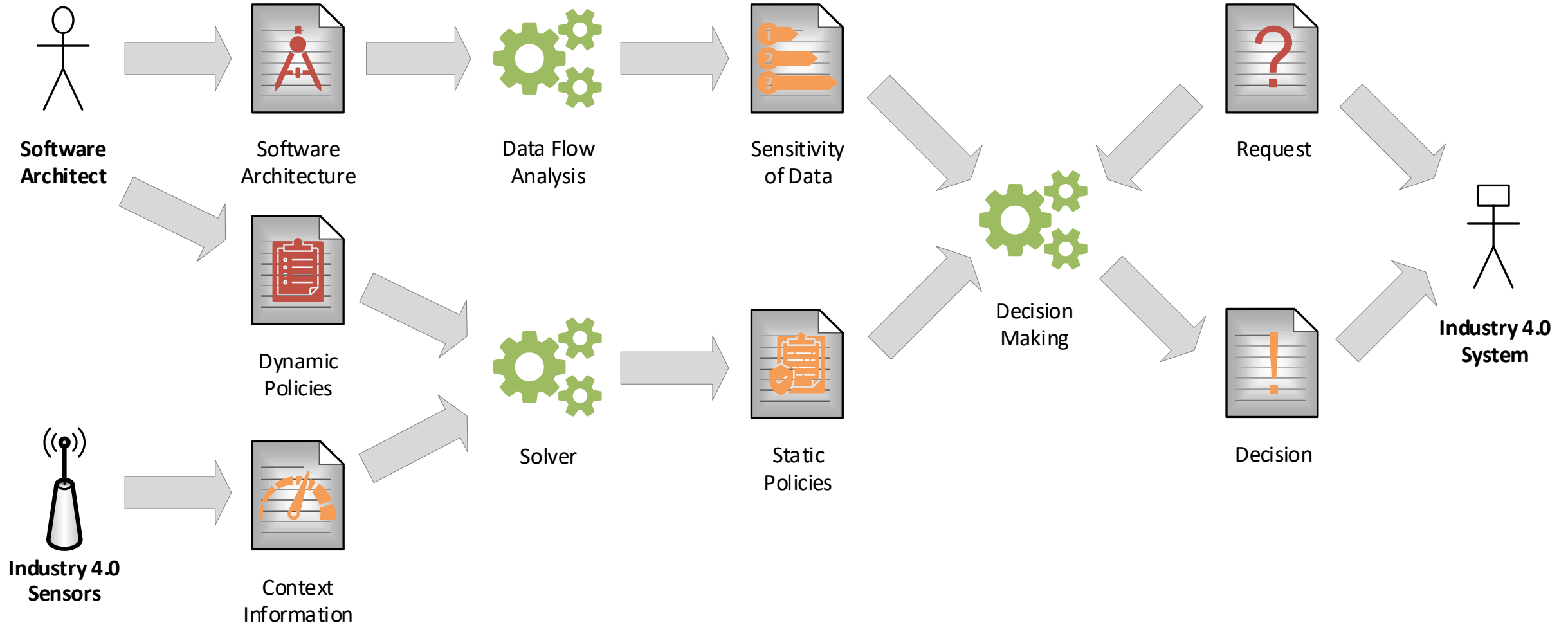
### Virtual Constraints

- Supervisor cannot access personal data of workers
- Supervisor cannot access sensitive personal data of late workers



# Trust 4.0 Approach

## Overview

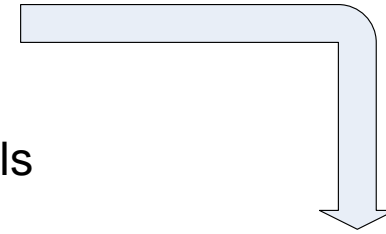


# Data Flow Analysis

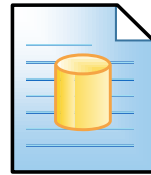
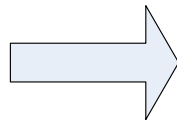
## Overview



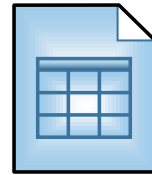
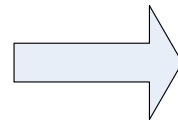
Analysis Goals



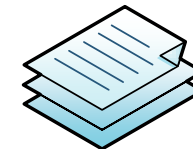
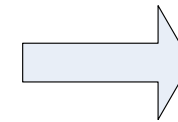
Architecture



Extended Architecture



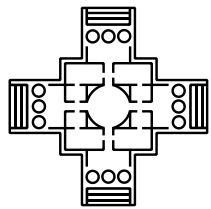
Analysis Model



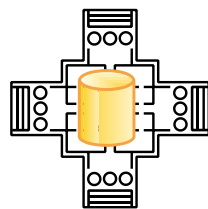
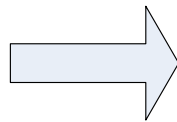
Logic Program



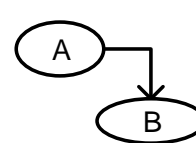
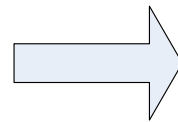
Results



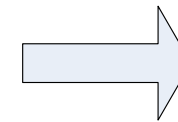
PCM Instance



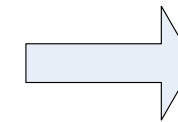
Data-Centric PCM Instance



Operations Model



Prolog Program

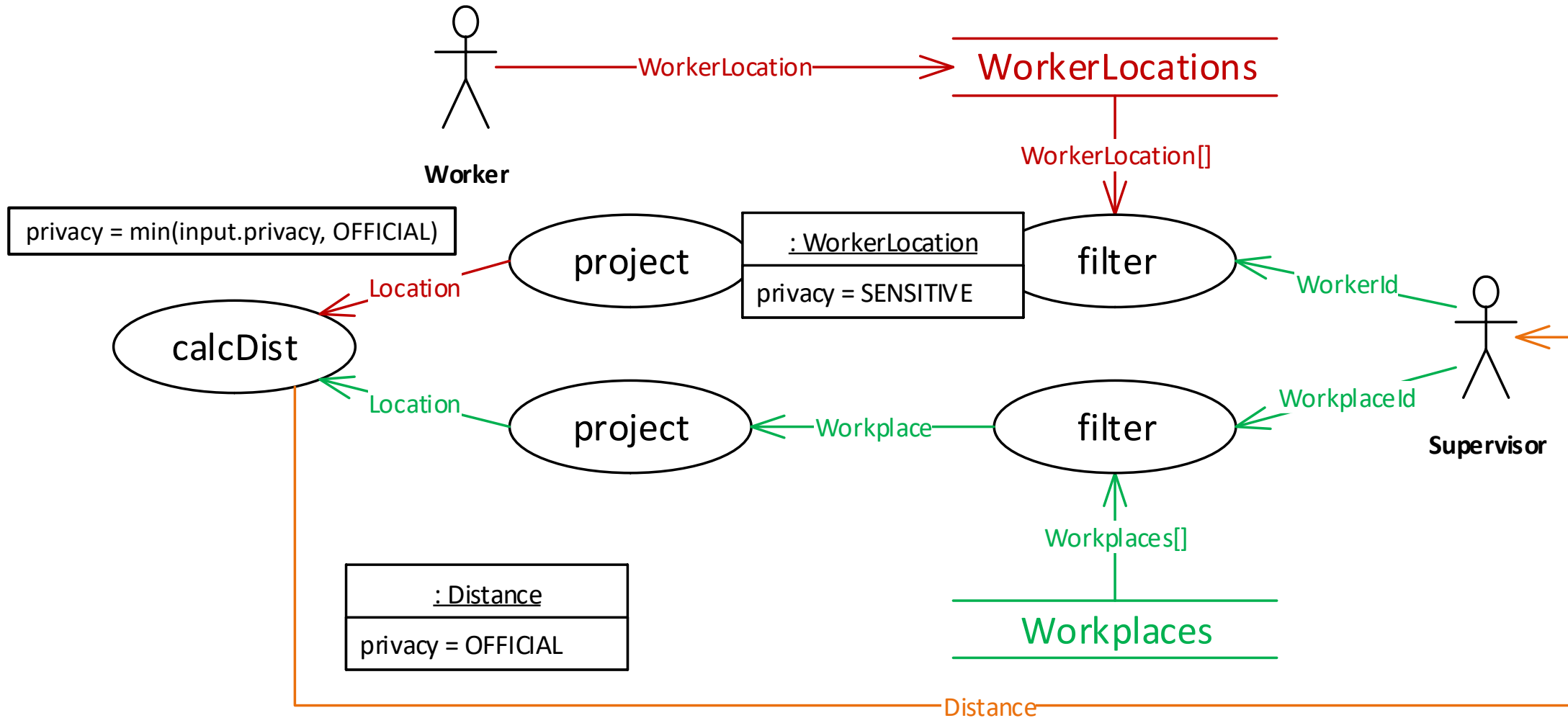


Query Result



# Data Flow Analysis

## Modeling and Analysis



# Data Flow Analysis

## Results

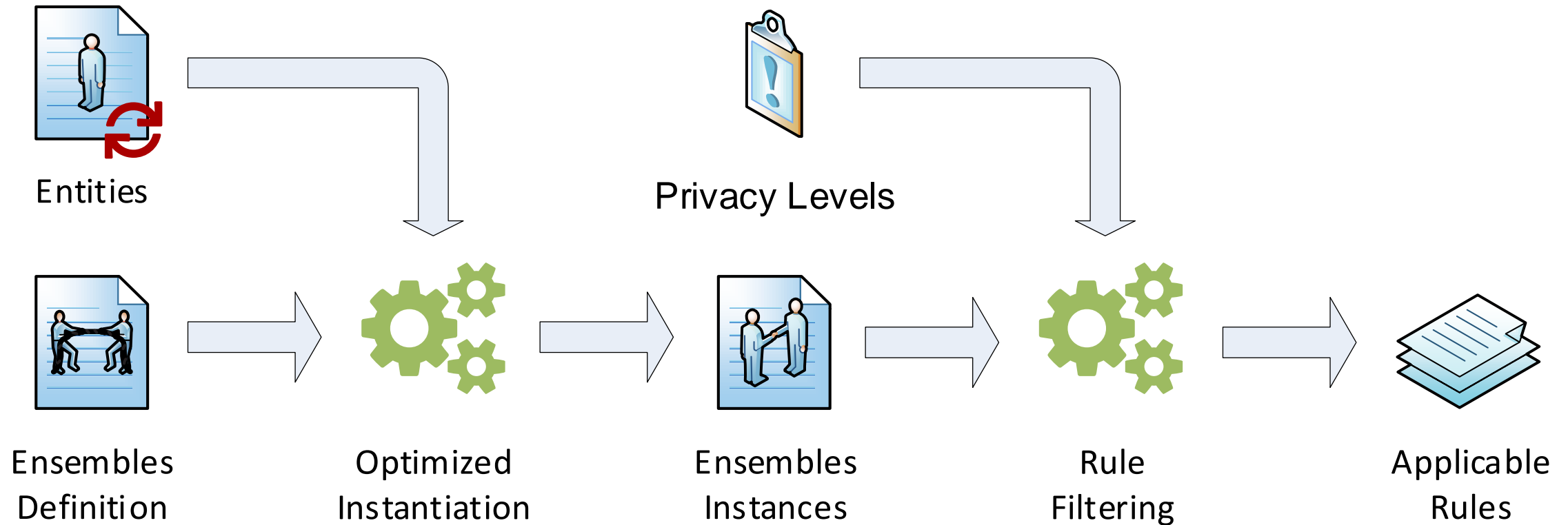


DataId	DataType	PrivacyLevel	EntryPoint
0	WorkerLocation	SENSITIVE	Worker UC1
1	WorkerId	NONE	Supervisor UC2
2	WorkerLocation	SENSITIVE	Supervisor UC2
3	Location	SENSITIVE	Supervisor UC2
4	Distance	OFFICIAL	Supervisor UC2
...	...	...	...



# Dynamic Policies

## Overview



# Decision Making

## ■ Grants

```
allow(shift.foreman, "read.personalData.phoneNo", workersThatAreLate)
```

```
allow(shift.foreman, "read.distanceToWorkPlace", workersThatAreLate)
```

## ■ Constraints

```
deny(shift.foreman, "read.personalData", workers, PrivacyLevel.ANY)
```

```
deny(shift.foreman, "read.personalData", workersPotentiallyLate, PrivacyLevel.SENSITIVE)
```

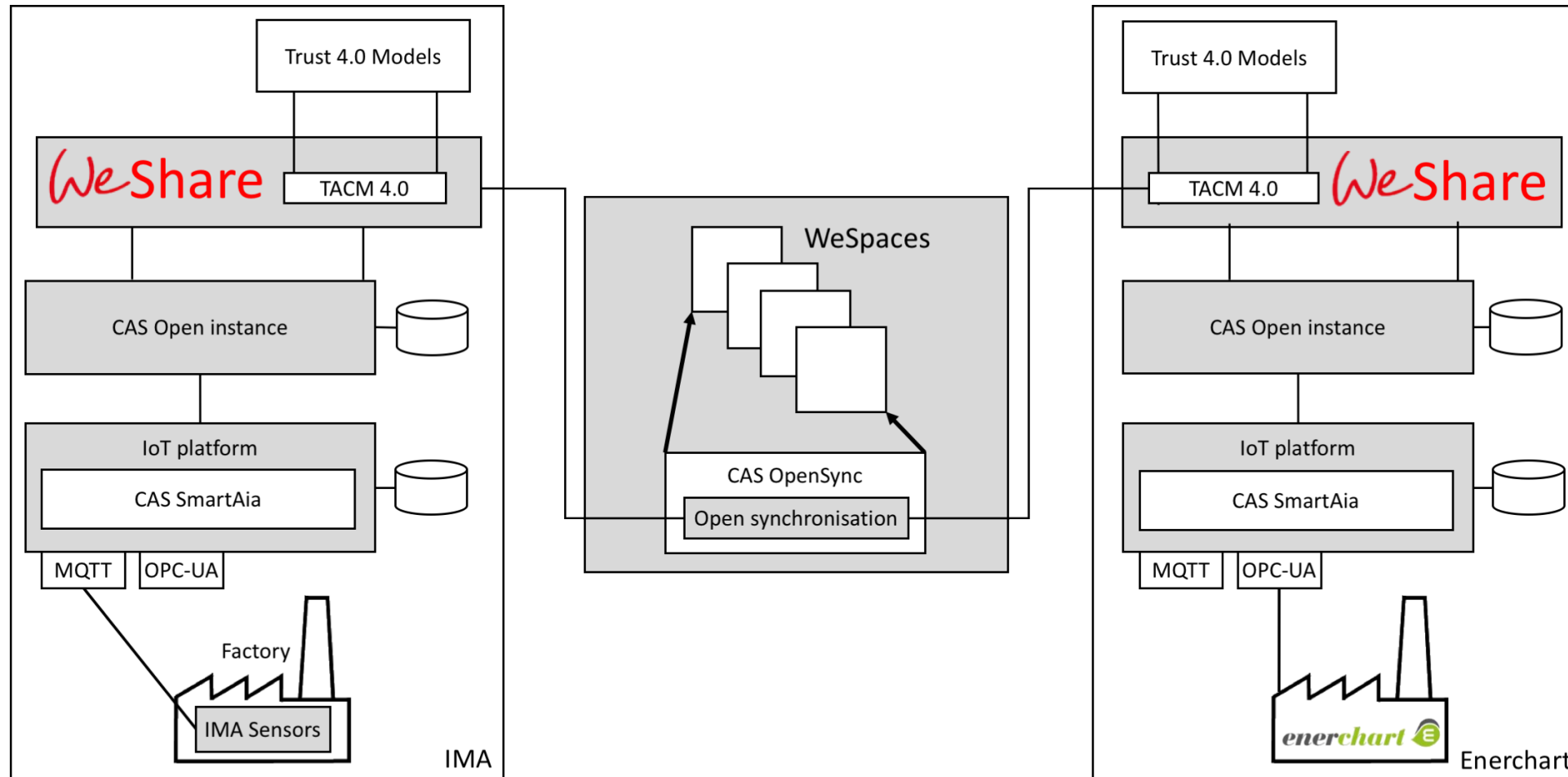
## ■ Privacy Levels

- Distance to work place, and phone number are official
- Remaining personal data of worker (e.g. date of birth) is private

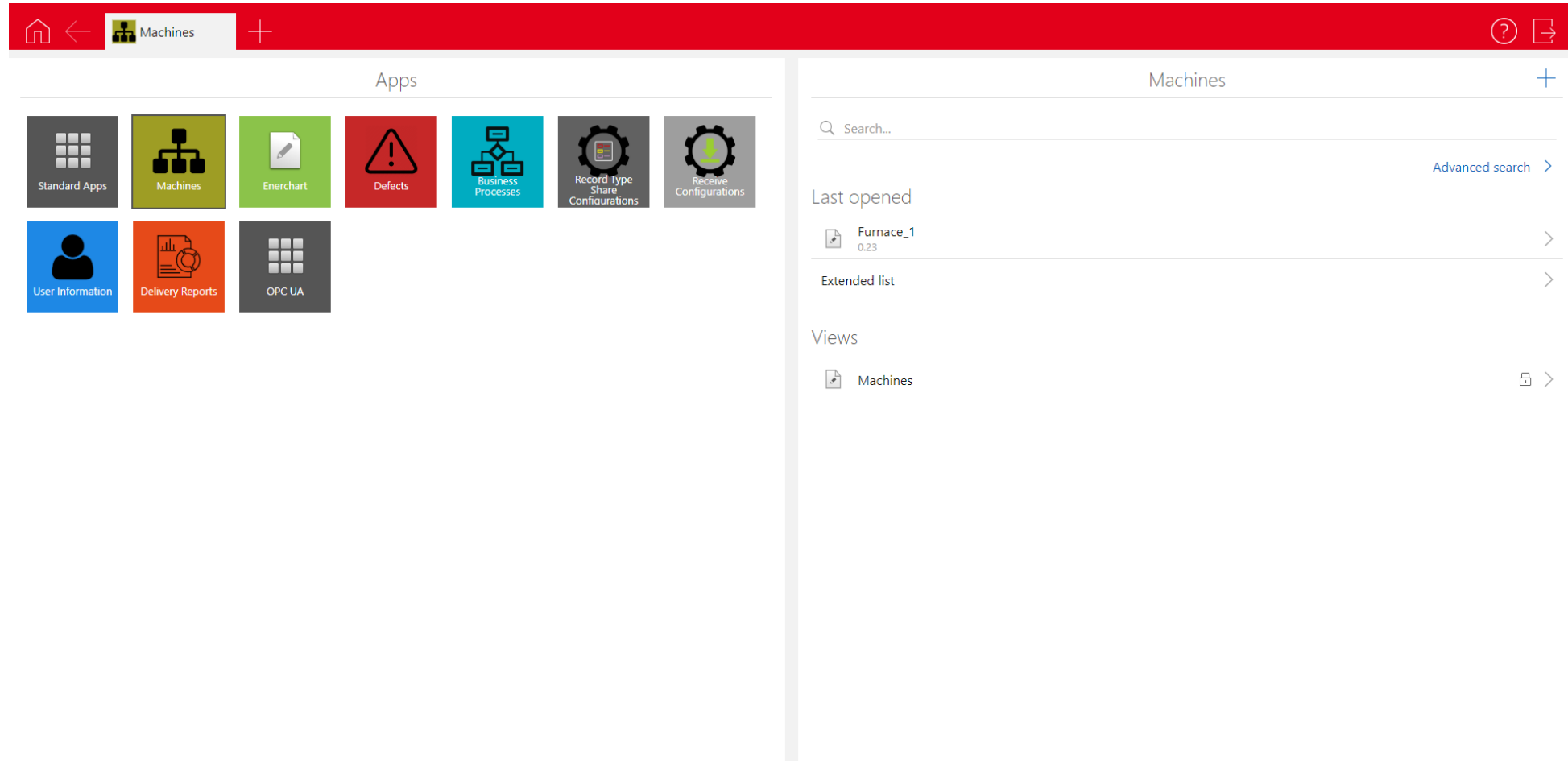




# Trust 4.0-enabled enforcement architecture



# WeShare for supply chains



# Privacy-oriented IoT data transfer (internal view)

Home < Machines + ? ↗

Last opened

- Furnace\_1 -0.05

Machine Edit

General

Identifier  
Furnace\_1

Temperature  
-0.05

KPI

Throughput  
0.90

Error Rate  
0.01

Additional information

Worker  
Karl-Heiz Schmidt

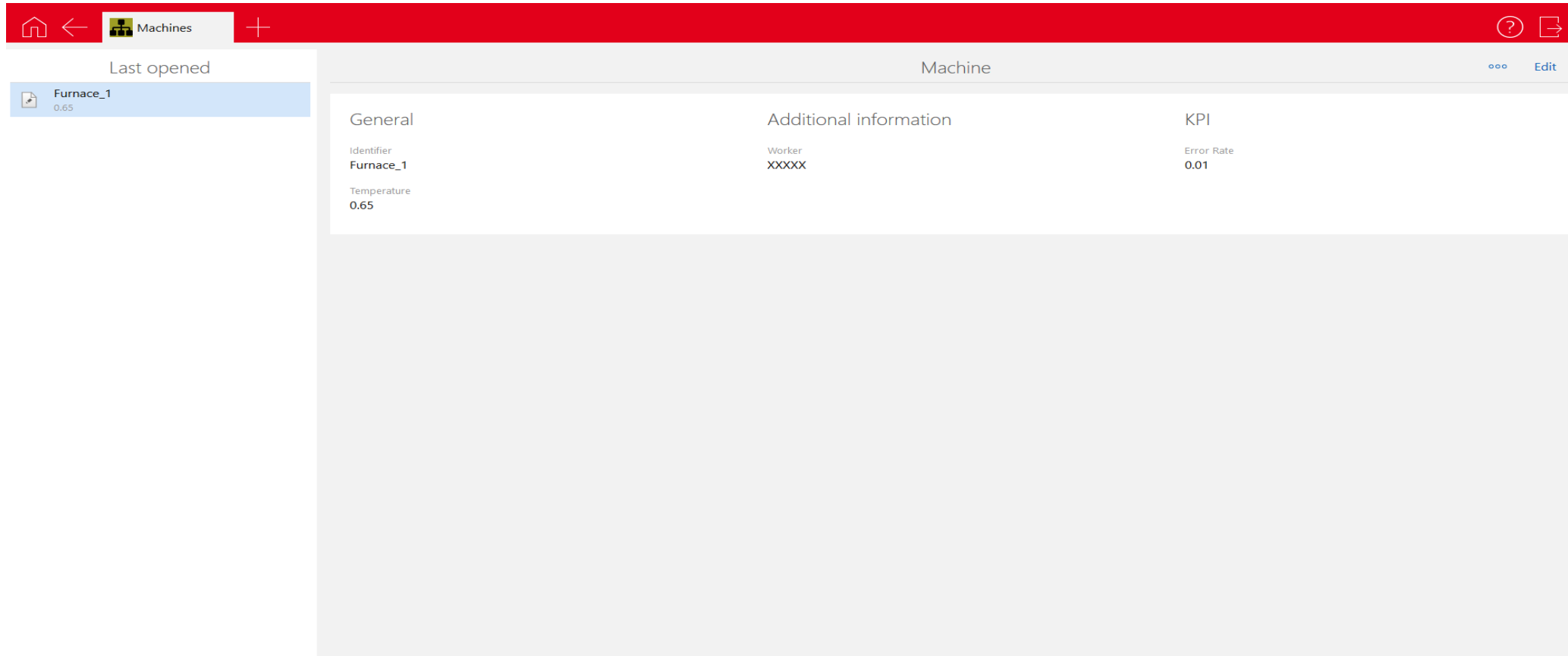
Dossier

- Delivery Report - B523F8311CBA37288B607C01010D8544  
Jun 3, 2019 - Delivery report for object with B523F8311CBA37288B607C01010D8544.
- Furnace\_1.Temperature  
Jun 3, 2019 - 3

Extended list



# Privacy-oriented IoT data transfer (restricted view)



General	Additional information	KPI
Identifier Furnace_1	Worker XXXXX	Error Rate 0.01
Temperature 0.65		



# Enerchart Charts based on restricted view

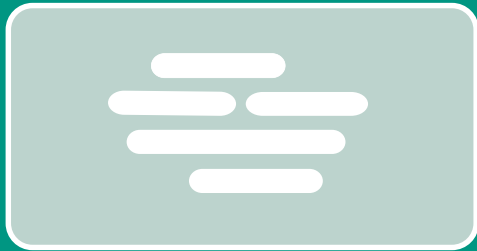


# Conclusion



## Incorporating trust in Industry 4.0 is challenging

- Rapid changes require reactions
- Complex communication patterns make policies complex



## Trust 4.0 supports aspect of access control

- Define bottom line security policies
- Define runtime policies considering context
- Evaluate policies on context changes



## Future Work

- Evaluation in industrial context
- Consideration of unforeseen context changes



# Image References

## General

- Cover Photo: Noelle Otto, cropped picture, free to use
- Facebook' Share Price Chart: P. Bhardwaj, Eight weeks after the Cambridge Analytica scandal, Facebook's stock price bounces back to where it was before the controversy, 2018. [Online]. Available:  
<https://www.businessinsider.de/facebooks-stock-back-up-cambridge-analytica-charts-2018-5> (visited on 16/03/2018)
- Icons: Font Awesome, changed color/background, CC-BY 4.0 License,  
<https://fontawesome.com/license/free>
  - Introduction: Factory, user with Shield, sync
  - Running Example: Lock (open/closed)
  - Dynamic Policies: Sync
  - Conclusion: Factory, shield, fast forward

# Image References

## Running Example

- Background vector created by vectorpocket - [www.freepik.com](http://www.freepik.com)
  - Living Room
- Background vector created by katemangostar - [www.freepik.com](http://www.freepik.com)
  - Waiting Area
- Business vector created by freepik - [www.freepik.com](http://www.freepik.com)
  - Office
  - Workers
- Technology vector created by macrovector - [www.freepik.com](http://www.freepik.com)
  - Factory
- Railway Clock made by Jahoe is licensed under CC BY-SA 3.0 and available on [Wikimedia Commons](https://commons.wikimedia.org/). Rearranged hands.



# Image References

## Approach Overview

- Icons made by Freepik (<https://www.freepik.com>) from Flaticon (<https://www.flaticon.com>) are licensed by CC 3.0 BY
  - Compasses, Speedometer, Numbering Icons
- Icons made by Dave Gandy (<https://www.flaticon.com/authors/dave-gandy>) from Flaticon (<https://www.flaticon.com>) are licensed by CC 3.0 BY
  - Cog Wheels Icon
- Icons made by Icongeek26 (<https://www.flaticon.com/authors/icongeek26>) from Flaticon (<https://www.flaticon.com>) are licensed by CC 3.0 BY
  - Clipboard Icons