Karlsruhe Reports in Informatics 2018,9
Edited by Karlsruhe Institute of Technology,
Faculty of Informatics
ISSN 2190-4782

Use Cases in Dataflow-Based Privacy and Trust Modeling and Analysis in Industry 4.0 Systems

Rima Al-Ali, Tomas Bures, Björn-Oliver Hartmann, Jiri Havlik, Robert Heinrich, Petr Hnetynka, Adrian Juan-Verdejo, Pavel Parizek, Stephan Seifermann, and Maximilian Walter

2018

KIT – University of the State of Baden-Wuerttemberg and National Research Center of the Helmholtz Association

Abstract

Fostering efficiency of distributed supply chains in the Industry 4.0 often bases on IoT-data analysis and by means of lean- and shopfloor-management. However, trust by preserving privacy is a precondition: Competing factories will not share data, if, e.g., the analysis of the data will reveal business relevant information to competitors. Our approach is enforcing privacy policies in Industry 4.0 supply chains. These are highly dynamic and therefore not manageable by 'traditional' rights-management approaches as we will stretch in a literature analysis.

To enforce privacy, we analyze two industrial settings and derive general requirements: (1) Lean- and shopfloor-management and (2) factory access control, both common in Industry 4.0 supply chains. We further propose a reference architecture for Industry 4.0 supply chains. We introduce the combination of Palladio Component Model (PCM) [23] and Ensembles [4] in order to analyze and enforce privacy policies in highly dynamic environments.

Our novel approach paves way for data sharing and global data analyzes in highly dynamic Industry 4.0 supply chains. It is an important step for efficiency of these supply chains and therefore one important cornerstone for the success of Industry 4.0.

Contents

1 Introduction

Supply chains in today's production processes are often highly distributed. Producers receive intermediate products from multiple suppliers that have multiple suppliers themselves. Producers reduce their storage capacity in favour of just in time production, which requires timely delivery of parts and low wastage. At the same time, customers want to track their customized product during the whole production process until they receive it. Industry 4.0 supports such scenarios by collecting and exchanging relevant information.

However, the participants of the supply chain do not want to exchange all information with all participants. For instance, the supply chain of a producer might contain two suppliers of the same part. The suppliers are therefore competitors, and they do not want to share information that gives an advantage to a competitor. Access constraints have to restrict information exchange. Often, these rules cannot be statically defined because the context of the information exchange can change dynamically. For instance, the role of an organization in the supply chain might change from a supplier to a producer, which requires more information shared with it.

Even if there are approaches to restrict information exchange by access control policies, they do not consider dynamic context changes that Industry 4.0 settings require. Additionally, a comprehensive list of requirements and relevant context information of such scenarios is not available.

To overcome this issue, we elicitate requirements and relevant context information from real world industrial settings. We do this by defining use cases for a data flow-based privacy analysis and enforcement in such settings. Additionally, we collect the state of the art regarding privacy analysis and enforcement approaches and check their abilities regarding the collected requirements.

The remainder of the paper includes the requirements for trust approaches in Chapter 2 that starts describing the Trust 4.0 reference architecture that guides the description of the two real-world industrial settings; namely, the settings of KPI sharing across supply chains and entities management within dynamic manufacturing process. Next, Chapter 3 describes the roles involved in the use cases and a detailed list of use cases that the Trust 4.0 will selectively tackle. Further, Chapter 4 describes the state of the art including approaches to confidentiality analysis, access control, enforcement, and data sensitivity. Finally Chapter 5 summarises the envisioned approach for trust enforcement to then let Chapter 6 conclude the technical report.

2 Requirements for Trust Approaches

Before describing the requirements, we specify a reference architecture for privacy preserving information exchange along supply chains. The reference architecture is necessary for specifying a common vocabulary and for describing all interfaces. Afterwards we describe requirements from real world industrial settings: Lean- and shopfloor-management as well as physical access control. Both settings apply in a distributed supply chain.

2.1 Trust 4.0 Reference Architecture

The requirements for trust approaches stem from two settings within the problem domain of privacy and trust in Industry 4.0 systems. Figure 2.1 describes the reference architecture that guides the requirements gathering phase according to two domains: (1) KPI *(Key Performance Indicators)* sharing across the entire supply chain within the context of lean- and shopfloor-management as Section 2.2 explains and (2) the physical access to buildings for entities management within dynamic manufacturing process as Section 2.3 describes.

The reference architecture shown in Figure 2.1 exemplifies a supply chain that shares information related to the local production business processes of each individual factory. The left-hand side of Figure 2.1 shows the software components in Factory 1 followed by Factory 2 to the right and multiple other factories that include Factory *n*. Each of these factories produces goods and is equipped with sensors that monitor the different processes involved in the production of those goods and other related business processes such as logistics or physical access to buildings. The different sensors in a factory feed the IoT platform through IoT interfaces – typically using communication protocols such as MQTT or OPC-UA[1] – which in turn aggregate the data for the local shopfloor-management system to show it to their users through its user interface. This helps users to monitor the status of the system as well as sharing information with other factories across the supply chain to improve the supply chain management by identifying weaknesses and opportunities of improvement.

Privacy and trust models govern the access control sub-component that allows or forbids the local shopfloor-management system to share data with other factories through the global shopfloor-management system at the top of Figure 2.1 according to the privacy of the data to be shared and the trust in the other factories. The local shopfloor

[1]The Message Queuing Telemetry Transport *(MQTT)* is a publish-subscribe messaging protocol working on top of the TCP/IP protocol and following an ISO standard[16]. The OPC Unified Architecture *(OPC UA)* is a platform-independent service-oriented architecture delivering a machine to machine communication protocol for industrial automation[9].

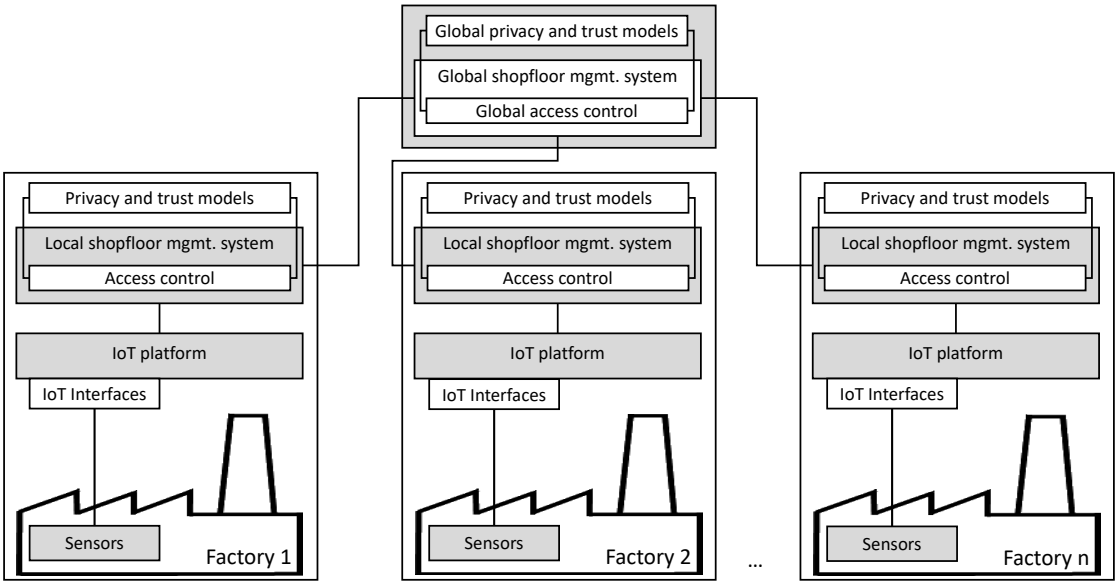

Figure 2.1: Reference architecture of the problem domain of privacy and trust in Industry 4.0 settings

management system uses its data to derive KPIs. KPIs are the information that this system shares with other shopfloor-management systems in other factories according to the privacy and trust models. If these KPIs are to be shared, the factory queries the global shopfloor management system that access the appropriate local shopfloor management systems according to its global access control mechanism that enforces the information exchange according to the global privacy and trust models.

In the following sections, we describe the requirements originating from the field of KPI sharing as well as the field of physical access control that uses the sensor data to decide about physical access and uses the physical location of people to decide about data sharing.

2.2 KPI Sharing Across Supply Chains

Lean- and shopfloor-management systems, such as ValueStreamer®[2], share KPIs and other data across supply chains *(SC)* according to the context of the data sharing operation as well as depending on the particular context of the business process involved in sharing such as the roles of the stakeholders involved, the time and date of the data sharing, the participant SC entity and its members, the specific time window for data sharing, the sharing location, or the provenance of the data across SC.

An example of organizations sharing KPIs across their supply chain include a car

[2]ValueStreamer® is a commercial product by the companies CAS software AG — co-authors of this paper — and Staufen AG. ValueStreamer® is a shop floor management system that delivers lean management principles and data sharing across the entire supply chain[5].

manufacturer as the central element of this supply chain reacting to the production issues of its multiple suppliers delivering gasoline systems, chassis system controls, brakes, tires, electrical systems, power-train control, and many other elements. The car manufacturer recognises its sourcing issues by identifying production problems of its suppliers according to their production machine error rates. Sharing these machine error rates data might entail privacy violations such as when these data are shared with competing organizations or if they contain personal data and are shared with a SC member that should not be allowed access. On the one hand the knowledge of error rates allows stakeholders to monitor, predict, and optimize the production process while on the other hand the error rates constitute sensitive information that have to be shared according to a set of privacy policies. The following functional and non-functional requirements try to address this dichotomy while enforcing appropriate levels of privacy and fostering trust.

2.2.1 Functional Requirements for KPI Sharing

The following functional requirements describe the necessary functionality for IoT data-driven and privacy-preserving lean- and shopfloor-management.

Requirement R1 – Data Sharing across the Entire Supply Chain

Users of lean- and shopfloor-management systems require efficient data exchange, i.e. KPI exchange, across the SC. The access and distribution of KPIs shall respect their data privacy level according to the involved stakeholders and the dynamic context of the data exchange. The data exchange should allow exchanging IoT data internally and across organisations including the KPIs stemming from the aggregated IoT data.

Requirement R1: Lean- and shopfloor-management systems have to let the user share data, such as KPIs, across the entire supply chain.

Requirement R2 – Privacy-Concerned Data Sharing

In addition to IoT data presenting no privacy challenges, there exists data with higher privacy levels such as personal data and data related to business processes. Personal data include data of employees and their working times in addition to data of suppliers. As for the business processes data, they could include data about the efficiency of the system, new developments, and data that might lead to extracting personal information about employees or data that is valuable for a company and therefore secret. Further, the system should consider the legal framework affecting the gathering, processing, backing-up, storage, and distribution of data in addition to how trust could be lost as a result of not respecting the privacy of these data.

Requirement R2: Lean- and shopfloor-management systems shall be able to enforce data privacy policies via allowing or forbidding data sharing across the supply chain.

Requirement R2.1 – Privacy-Aware Analytics and Predictions

Data analytics or data-based predictions aggregate different data and KPIs to predict critical situations, provide decision support, or discover patterns so as to make recommendations or predictions. However, these algorithms should not be able to reveal information in a way which conflicts with privacy policies.

Requirement R2.1: Lean- and shopfloor-management systems should be able to enforce data privacy policies, even in the context of analytics or predictions resulting of the combination of different data sources and KPIs.

Requirement R2.2 – Respecting the Legal Framework

The protection of the data should respect the particular legal framework. In the European Union, computing systems must respect the General Data Protection Regulation *(GDPR)*. In other countries, other comparable laws must be respected.

Requirement R2.2: Lean- and shopfloor-management systems shall be able to enforce data sharing privacy policies that respect relevant legal frameworks.

Requirement R2.3 – Privacy Awareness in Business Processes

In accordance with particular processes, data sharing may be allowed or forbidden. The context of business processes greatly affects how information is shared. For example a machine maintenance operator will get access to machine only within the context of an authorised maintenance operation but not be allowed to access those data otherwise.

Requirement R2.3: Lean- and shopfloor-management systems shall be able to enforce data sharing privacy policies with regards to executed business processes.

Requirement R2.4 – Role-Dependent Privacy

Data access depends on the role of the stakeholder trying to access the data. The role itself might depend on organisational structures, specific context of the process being executed in that particular time and other factors. For example, the role of stakeholders involved in a business process as senior managers might give them access to some data while a machine operator might not be entitled to access them. An exception might be that for a particular time window and for a machine that requires maintenance the operator has access to the data in order to maintain the machine. This shows that the sharing permissions are very dynamic. They evolve over time like in this case or in cases granting the right to erasure or right to be forgotten.

Requirement R2.4: Lean- and shopfloor-management systems shall be able to enforce data sharing privacy policies with regards to the roles of the participants in the executed business process.

Requirement R2.5 – Enforcing Privacy along Organisational Structures

Data is shared within organizations across their organizational structures and beyond organizational structures. Organizational secrets can often be shared with subsidiary

or holding companies as they pertain to the same organizational structure and are not allowed to share beyond organizational borders. The organizational context entails whether a stakeholder can exchange particular data according to the role of the participating organizations. This is challenging in Industry 4.0 ecosystems with roles, organizations, and the entire SC members and configuration changing rapidly over time.

Requirement R2.5: Lean- and shopfloor-management systems shall be able to enforce data sharing privacy policies with regards to the structure of the organisation sharing the data.

Requirement R2.6 – Data Sharing according to the Time-Related Context

Time and time-related constraints determine the period during which stakeholders can exchange particular data and its expiration time. These constraints might depend on the order of actions within a business process such as the already mentioned example of procurement in Requirement R2.3. For example, contracts between supply chain members usually specify confidentiality agreements for a specific period of time defining what can be shared, how, and with whom. Additionally, some data should be deleted after a period of time or after this data served the purpose for which it has been collected.

Requirement R2.6: Lean- and shopfloor-management systems shall be able to enforce data sharing privacy policies with regards to the time-related context of the executed business process.

Requirement R2.7 – Location and Privacy

If a machine operator has physical access to a machine, then the operator might also have access to the machine data. This might not be allowed, if the same operator does not have the physical access, e.g. because he/she is at home.

Requirement R2.7: Lean- and shopfloor-management systems shall be able to enforce data sharing privacy policies with regards to the location-related context.

2.2.2 Non-functional Requirements for KPI Sharing

Non-functional requirements are an important part of the commercial use of privacy-preserving mechanisms, as they increase the acceptance among the users of the mechanisms. The following non-functional requirements have been included. Furthermore, these requirements are only discussed in the event of major deviations since they must be taken into account for the scientific investigation, but do not play a central role. This is a frame of economic exploitation of the approaches to consider more closely.

Requirement NFR1 – Performance

KPI data shared from lean- and shopfloor-management systems should be timely ready for other systems to build on top of that data. For example, according to the experience gathered in the span of these and previous projects with regards to the throughput per

hour, data objects such as related KPIs shared across worldwide supply chains require to be readily available for other SC stakeholders within 10 minutes.

Lean- and shopfloor-management systems have to take the decision to allow data access or not within the same timeframe and therefore need a certain performance.

Requirement NFR 1: Lean- and shopfloor-management systems shall compute privacy-related mechanisms in less than 5 minutes in a state-of-the-art workstation.

Requirement NFR2 – Platform-independent Architecture

Industry 4.0 settings use sensors from different vendors and potentially proprietary platforms. Users require data and application portability, which entails respecting Industry 4.0 standards while preventing sensitive data reaching unauthorised parties independently from which stakeholder implements the interfaces to vendor-specific components.

Requirement NFR 2: Lean- and shopfloor-management systems shall platform-independently enforce privacy.

Requirement NFR3 – Secure Communication

Enforcing privacy is difficult without secured communication. Therefore, lean- and shopfloor-management systems shall deliver secured communication.

Requirement NFR 3: Lean- and shopfloor-management systems shall share data over secured protocols.

Requirement NFR 4 – Reliability

Modern distributed supply chains strive for a high delivery reliability. This reduces storage costs. The prerequisite is that all components of the supply chain have a high degree of reliability with regard to quality and availability.

Requirement NFR 4: Lean- and shopfloor-management systems shall be reliable in terms of availability and result quality.

2.2.3 Summary Requirments for KPI Sharing

Functional and non-functional requirements, such as contextual dependence on processes, jurisdictions, location, time, organizational structures, roles, as well as performance, platform independence, secure communication, and reliability, are key components of privacy-preserving mechanisms for lean- and shopfloor management in distributed supply chains.

All requirements apply at the same time and must be taken into account dynamically since they can already be dynamic in themselves.

2.3 Entity Management within Dynamic Manufacturing Process

This section describes requirements based on a scenario[3] of entity management in future dynamic manufacturing processes. The *entity* term here refers to human resources but also to other facilities (factory, halls) and equipments (dispensers of protective equipment) or even processes.

2.3.1 General Scenario Settings

Human resources management in real time is a foundation of high quality manufacture provision. The aim of the scenario is to develop models in order to ensure security and trust in continuous manufacturing processes. Within the manufacturing processes the manufacturing chains producing specific products will by defined. The continuity of the manufacturing processes is ensured if particular positions in the period of time are assigned according to position definition within the organization structure and the respective people and other entities assigned in the positions are given respective permissions needed to properly execute their tasks. Filling in the position is further determined by respective qualification requirements on the position within organization.

Figure 2.2 shows an example setup of the organization structure (entities taking part in the manufacturing process are listed in Table 2.1). The figure shows a production area (a factory), which is further divided into several halls. Each hall is used for a specific manufacturing performed by several workers and observed by a single foreman.

Setup of a Work Shift

The manufacturing process is performed in shifts. A time line of a particular shift is shown in Figure 2.3 (Table 2.2 list entities taking part in the shift).

Each shift requires a foreman and a given number of workers, each with a certain skill set. If a particular worker does not arrive in the shift, a replacement can be called in. However this requires time. As the shift cannot start without all the workers being present, it is desirable that the foreman is notified in advance if a particular worker is missing at the workplace before the shift.

If the shift set up needs to be complete at the start (or in defined time in advance) of the shift activities, we must monitor workers. In the particular shift, we need a single Foreman-V, four workers VD1-4, working in the hall Hall-1. If we monitor status or occurrence of individual entities in terms of time and space, e.g. presence in the hall at time T1, we can expect readiness of the shift 1 at the time T3 when the shift activities need to begin. If the composition of the entities in the time T1 is not complete the system generates an inquiry (SMS, email, call) urging the original entity, asking for confirmation. If the availability is not confirmed then the process replacing the missing entity by the standby entity is initiated.

[3]The scenario is based on activities of IMA – co-authors of this paper

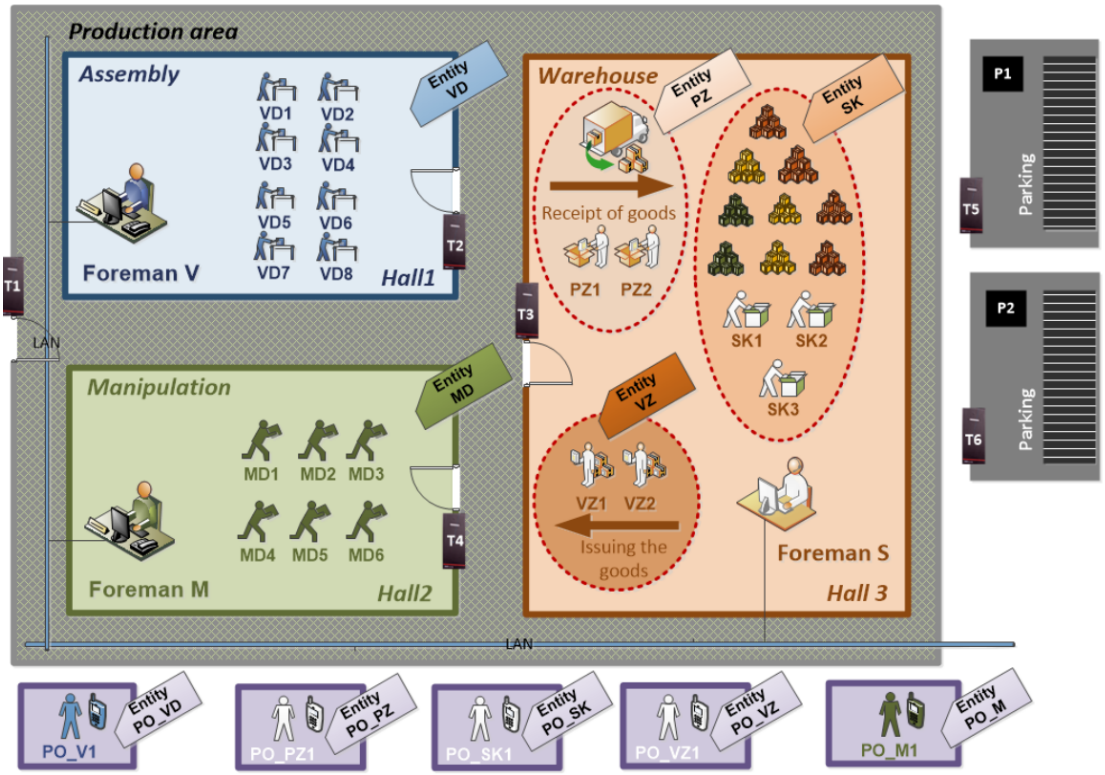

Figure 2.2: Use-Case Overview

2.3.2 Functional Requirements for the Entity Management (EM) Scenario

In Figure 2.2 and Table 2.2, we depicted EM in terms of activities of all the entities. Based on that we have to make elicitation of use-case requirements in order to ensure that all activities can be performed with "trust and privacy-preserving emphasizing the dynamicity" of the activities/processes. On the other hand not all requirements can be implemented and validated during demonstration because of limited size of the system and limited number of entities.

Requirement R3 – Trust Model Implementation Validation

When the trust model is invented, the implementation of it has to be validated. The uneasy implementation should either discourage or block the successful system improvements expected of the model.

Requirement R3: Entity Management within Dynamic Manufacturing process should be easily implementable within identification system at the client.

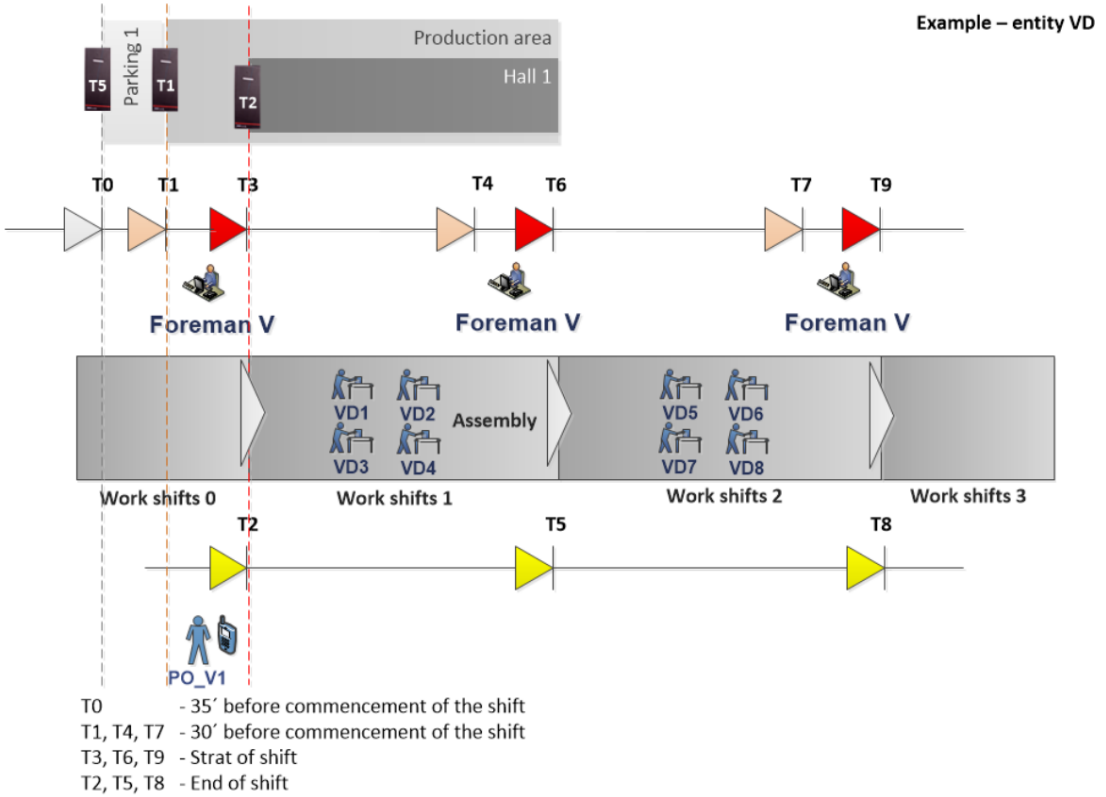

Figure 2.3: Shifts sequence in the time line

Requirement R4 – Secure Communication Among Access Control System (ACS) Components

The ACS platform consists of number of elements which communicate via various interfaces. Each communication channel is a potential weak point where data may be misused. Secure links are a necessary assumption to build trust model on top of that.

Requirement R4: Entity Management within Dynamic Manufacturing process shall provide secure communication within access control system at the client.

Requirement R5 – Protection of Hardware against Intrusion

In ACSs the sensitive data come usually into existence in the hardware, i.e. readers or terminals. Sophisticated methods to hack the system aim also at the hardware employing an untreated defect in the hardware design, e.g. eavesdropping of inter-core communication or physical connection to ports of microcontrollers.

Requirement R5: Entity Management within Dynamic Manufacturing process have to provide efficient protection of the hardware components against intrusion.

Requirement R6 – Privacy Awareness within whole EM

This requirement stands on the top and it means that each entity which uses any system component (computers, mobile, kiosks, work tools, access control readers/gates etc.) is familiarized how to use it, what kind of data are linked with the component, how to take care of UI, how to behave in unexpected events.

Requirement R6: Entity Management within Dynamic Manufacturing process shall ensure that each entity which uses any system component is familiarized how to use the system in regard to privacy awareness.

Requirement R7 – Role-Dependent Privacy

As every entity has a specific role within the system meeting different data (records) also the attitude towards privacy needs to be different. The foreman obtaining phone numbers, sending messages has different value of privacy in his/her "hands" then worker reading product lists involving technical data or failure rates or country of origin.

Requirement R7: Entity Management within Dynamic Manufacturing process shall provide privacy to every entity which is specific to role that entity plays within the system.

Requirement R8 – Location-Dependent Privacy

This requirement is linked to R5, e.g. the foreman has one set of data in his office and other one when entering the work place handling with products or components. At both sites the privacy is managed by different way.

Requirement R8: Entity Management within Dynamic Manufacturing process shall provide privacy to every entity which is specific to the location where the entity works within the system.

Requirement R9 – Enforcing Privacy by Entity Occurrence

If an entity enters a place in the factory from public place or changes the work-places within the factory then the privacy has to be strongly considered according to presence in order to prevent intentional/unintentional misusing data about parts, products, tools or work place.

Requirement R9: Entity Management within Dynamic Manufacturing process have to provide privacy enforcement to the entity if the entity changes the work-places within the factory.

Requirement R10 – Entities Data Sharing Schedule

This requirement is linked to system configuration (one of management function) where scheduling of sharing data among entities is crucial functionality. According to schedule set up for example the foreman may see contacts of assigned workers only several minutes before the scheduled start of the shift.

Requirement R10: Entity Management within Dynamic Manufacturing process have to ensure the entity can share or have data at disposal by the schedule at the right time & place.

Requirement R11 – Issue/Event/Process strictly demarcated by Time Stamps

The requirement is presented in figure 2.3, and expresses strictly when the process begins and when it ends and thus the system has to control online the fulfillment of the tasks within individual time windows.

Requirement R11: Entity Management within Dynamic Manufacturing process have to ensure the system can control online the fulfillment of the tasks within set time windows.

Requirement R12 – Non-Redundancy

The system offers to the entity only data absolutely necessary for the single process, e.g. the system pushes to the foreman the backup workers' contacts only when the regular worker is missing and backup entity is being looked for. When a substitute is found the backup contacts are discarded of the process.

Requirement R12: Entity Management within Dynamic Manufacturing process shall provide or require only absolutely necessary data which belong to specific process or activity.

2.3.3 Non-functional Requirements for Entities Management Use Case

Requirement NFR5 – System Performance

This is rather general but very important requirement also connected with scope of the system. The system will be designed in respect to number of entities, gates, work places, complexity of the processes etc. The bigger volume of data will be going through the system the higher performance of the system or system components is required. For example if number of ID readers at the gates approaching the limit which the master may technically handle then the number of masters has to be increased. Or if number of process records is expected extremely high then the capacity of the interfaces needs to be designed in this regard.

Requirement NFR5: Entity Management within Dynamic Manufacturing process have to provide demanded system performance in order to ensure running of all required processes.

Requirement NFR6 – Maintainability

In case a failure of the system we have to ensure prompt fixing of it. If the maintenance is technically difficult or inaccessible in short time then the reliability of the system is getting low.

Requirement NFR6: Entity Management within Dynamic Manufacturing process shall allow technically feasible maintenance operation.

Requirement NFR7 – Comfort, Usability

All system components have to be easily accessible and controllable by workers/foremen. E.g., if the terminal has a keyboard, display or other kind of user interface then it has to be directly controllable by a worker/foreman with protection gloves.

Requirement NFR7: Entity Management within Dynamic Manufacturing process shall provide to user a certain level of comfort when he/she handles the system components as user interfaces, devices and tools.

Requirement NFR8 – Operability

The access control system is composed of number of components. Using these components and their functionalities the use case is executed. These components have to be able to work together to achieve "common tasks".

Requirement NFR8: Entity Management within Dynamic Manufacturing process have to ensure an ability of the system components to work together.

Requirement NFR9 – Legal Framework Compliance

Respective contracts need to be clinched. The contracts have to deal with related law provisions linked to identity, security, data protection etc.

Requirement NFR9: Entity Management within Dynamic Manufacturing process shall be compliant with trust and privacy specific law regulations.

Requirement NFR10 – Reliability, Availability, Serviceability, Manageability

This set of requirements refers four separate but related characteristics of a functioning system. For our use case we will focus on configuration and control how the services are available, probability that a component, subsystem or full system, will accomplish its assigned task within a specified time etc.

Requirement NFR10: Entity Management within Dynamic Manufacturing process shall be developed in order to achieve RASM kind of non-functional behavior within the whole ACS system.

Requirement NFR11 – Physical Protection

Also connected to R3, the physical (even mechanical) protection, e.g. locked room or rack, avoids the access to the hardware and safe the hardware against connection to electronic boards or data interfaces. The reliable mechanical casing of the system components could be also considered in this requirement.

Requirement NFR11: Entity Management within Dynamic Manufacturing process will be integrated within the access control system which have to be physically protected in order to avoid access to the hardware components.

Table 2.1: Catalogue of entities linked to the model on Figure 2.2 related:

Entity	**Entity Type**
Foreman V	Foreman
Foreman M	Foreman
Foreman S	Foreman
VD1	Worker
VD2	Worker
VD3	Worker
VD4	Worker
VD5	Worker
VD6	Worker
VD7	Worker
VD8	Worker
MD1	Worker
MD2	Worker
MD3	Worker
MD4	Worker
MD5	Worker
MD6	Worker
PZ1	Worker
PZ2	Worker
SK1	Worker
SK2	Worker
SK3	Worker
VZ1	Worker
VZ2	Worker
PO_V1	Worker - Standby
PO_PZ1	Worker - Standby
PO_SK1	Worker - Standby
PO_VZ1	Worker - Standby
PO_M1	Worker - Standby
Production area	Space
Parking1	Space
Parking2	Space
Hall 1	Space
Hall 2	Space
Hall 3	Space
Assembly	Process
Manipulation	Process
Warehouse	Process
T1	Gate
T2	Gate
T3	Gate
T4	Gate
T5	Gate
T6	Gate
Shift 1	Shift
Shift 2	Shift
Shift 3	Shift

Table 2.2: Relationship to shift

Entity	**Entity Type**
Foreman V	Foreman
Shift 1	Shift
Assembly	Process
VD1	Worker
VD2	Worker
VD3	Worker
VD4	Worker
PO_V1	Worker - Standby
Parking1	Space
T5	Gate
Production area	Space
T1	Gate
Hall 1	Space
T2	Gate

3 Use Cases

Use cases are a way to define requirements for a system with respect to interactions between the system and its users. In this section, we describe typical use cases originating from the domains described above. The use cases are about the whole supply chain management system and do not only describe access control. This is useful to better understand the requirements about access control given in Chapter 2 and the according context information.

The use cases combine both scenarios of KPI sharing and physical access control. This also covers interactions between these use cases. We use a simplified version of the fully dressed use case template of Cockburn [7] to describe the use cases.

3.1 Use Case Roles

The following use cases describe their flow of information and involve several roles working within organisations across the supply chain, on the example of Factory A, B and C. The use cases follow the reference architecture shown in Figure 2.1 in Chapter 2. The following roles apply:

- *Worker*: the worker operates a machine that transmits sensor data and KPIs. The worker participates with other workers in shifts overseen by a foreman that last for a certain period of time at various locations or production lines.
- *Foreman*: the foreman plans the shift and deals with any incidents that might occur.
- *Factory*: factories are part of the supply chain as a suppliers and consumers. If, for example, Factory A produces a product for Factory B then Factory A is supplier of Factory B and Factory B is a consumer of the products of Factory A. If Factory C is a consumer of products from Factory B, then Factory B is a supplier of Factory C.
- *Analyst*: the analyst performs the lean- and shopfloor-management in each factory by modelling the factory KPIs and analysing the monitoring results of those KPIs.
- *Board*: Factory A, Factory B, and Factory C have agreed on using a global supply chain management system and have accordingly founded a board to carry out global lean- and shopfloor-management tasks.
- *Domain Expert*: the domain expert creates models and analyses privacy requirements.

3.2 List of Use Cases

We created 5 use cases. Figure 3.1 shows the actors for every use case and the relation between the use cases. Entities appearing in the use-cases (plus relations among these entities) are shown in the domain model in Figure 3.2.

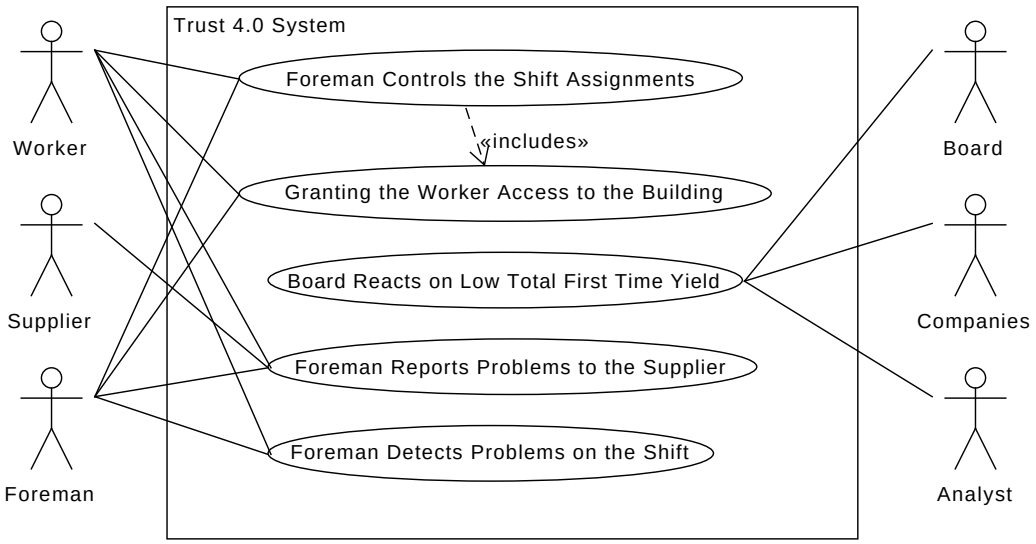

Figure 3.1: Use Cases Overview

3.2.1 UC 1: Foreman Detects Problems on the Shift

Scope Assembly Line Production

Preconditions

- The domain expert has defined the process and the restrictions
- The work schedule is available and the restrictions are loaded
- External reports from the supply chain management about bad quality arrived
- The Physical Access Control System (PACS) detected that the foreman accessed the workplace

Success End Condition The problem in production can be identified.

Failed End Condition The problem in production can not be identified.

Actors

- Worker
- Foreman

Trigger Factory-System decides the problem is within the production line

Description

1. The Foreman gets information about problem in the production line
2. The Foreman sees the work schedule of her/his workers
3. The Foreman addresses the problem in production

Extensions

2a *worker was in the shift with the faulty time at least 5 times*:
   1. The Foreman sees name of the worker
   2. The Foreman addresses the particular worker

Relation to Requirements The following requirements for KPI sharing across supply chains are reflected in the use case:

- Requirement R1 – Data Sharing: KPIs are transmitted.
- Requirement R2 – Privacy, Requirement R2.1 – Analysis and Predictions, Requirement R2.2 – Legal Framework: Depending on the jurisdiction, only aggregated values that do not allow for inferences about personal data or all data are transmitted.
- Since the foreman has to be in place and because he only receives information about the workers in his team, the same requirements are affected as in use case 4.

The following requirements for factory access control are reflected in the use case:

- R6 – Privacy awareness within whole EM
- R7 – Role-dependent privacy
- R9 – Enforcing privacy by Entity occurrence

3.2.2 UC 2: Foreman Reports Problems to the Supplier

Scope Assembly Line Production

Preconditions

- The domain expert has defined the process and the restrictions
- External product is faulty
- The PACS detected that the foreman and the worker are at their work places

Success End Condition The supplier gets informed

Failed End Condition The supplier does not get informed

Actors

- Worker
- Foreman
- Supplier

Trigger Worker identifies a faulty item used in production

Description

1. The worker informs the foreman about the faulty item
2. The foreman informs the external supplier

Extensions none

Relation to Requirements The following requirements for KPI sharing across supply chains are reflected in the use case:

- Requirement R1 – Data Sharing: The deterioration of quality is transmitted from Factory B to Factory A.
- Requirement R2 – Privacy, Requirement R2.3 – Processes: data on the quality of the process will only be transmitted if the agreed quality is undercut. Otherwise, the information is confidential.
- Requirement R2.4 – Role, Requirement R2.6 – Time, Requirement R2.7 – Location: The foreman is allowed to share the information because he has the role of foreman. He is also at the location of the shift that is in the fault process, and at the time the fault occurs.

The following requirements for factory access control are reflected in the use case:

- R6 – Privacy awareness within whole EM

- R7 – Role-dependent privacy
- R8 – Location-dependent privacy
- R11 – Issue/event/process strictly demarcated by time stamps

3.2.3 UC 3: Board Reacts on Low Total First Time Yield

The First Time Yield is the number of good units produced divided by the number of total units going into the process. It is used in many analysis.

Scope Supply chain management

Preconditions

- The domain expert has defined the process and the restrictions
- Every company calculate the first time yield for its own
- The first time yield is shared with the board

Success End Condition The companies with the two lowest yields are informed

Failed End Condition No company is informed

Actors

- Board
- Analyst
- Companies

Trigger Low First Time Yield is recognized

Description

1. The Board informs the Analyst of the Board about the low yield
2. The Analyst finds the companies with the two lowest yield
3. The Analyst informs the Board about the two companies
4. The Board informs the two companies

Extensions none

Relation to Requirements The following requirements for KPI sharing across supply chains are reflected in the use case:

- Requirement R1 – Data Sharing: The initial yield is transmitted to the board.
- Requirement R2 – Privacy: The board transmits information to individual factories (without informing other factories).
- Requirement R2.1 – Analytics and Predictions: Global analyzes are performed by the Board.

3.2.4 UC 4: Granting the Worker Access to the Building

Scope Physical Access Control System (PACS)

Preconditions

- The domain expert has defined the process and the restrictions
- The PACS has loaded the process and restrictions
- The PACS detected that the foreman accessed the workplace

Success End Condition Access for worker has been granted

Failed End Condition Access for worker has not been granted

Actors

- Worker

Trigger Arrival phase of shift started (30-45 min before shift)

Description

1. The system notifies the worker on how to access the parts of the compound for the actual shift.
2. The system grants the worker access to the building

Extensions none

Superordinates UC 5

Relation to Requirements The following requirements for KPI sharing across supply chains are reflected in this use case:

- Requirement R1 – Data Sharing: The access control receives data from different sensors at the access points of the areas of the factory.
- Requirement R2 – Privacy: The foreman does not have access to personal data
- Requirement R2.2 – Legal Framework: Depending on the legal area, the evaluation of the position of the foreman is not permitted or permitted, because of privacy rules.
- Requirement R2.3 – Business Process: Depending on which production line is serviced (and whether the process is normal production - and not, for example, an incident), the worker has access to different areas.
- Requirement R2.4 – Role: Whether a person has the role of worker or the role of foreman affects the access and thus the data flow.
- Requirement R2.5 – Organizational Structures: A worker is part of the foreman's team. That the roles are based on the organizational structure in this scenario.
- Requirement R2.6 – Time: The shift takes place at a certain time. At other times, the worker can not enter the designated area.
- Requirement R2.7 – Location: The shift takes place on a specific production line. This one has a place. Depending on the location of the foreman, access to the area of the production line may or may not be allowed.

The following requirements for factory access control are reflected in the use case:

- R3 – Trust model implementation validation
- R4 – Secure communication among access control system (ACS)components
- R5 – Protection of hardware against intrusion
- R11 – Issue/event/process strictly demarcated by time stamps

3.2.5 UC 5: Foreman Controls the Shift Assignments

Scope Shift management

Preconditions

- The domain expert has defined the process and the restrictions
- The PACS has loaded the process and restrictions
- Shift assignments are created.

Success End Condition Shift successfully started, proceeded and ended.

Failed End Condition Shift does not successfully started, proceeded or ended.

Actors

- Worker
- Foreman

Trigger Arrival phase of shift started (45 min before shift)

Description

1. The foreman is at his/her office 45 minutes before the shift
2. Worker is at the factory compound 30 minutes before the shift
3. System verifies this by reading workers location (once the worker is at the compound, the foreman is granted to observe the worker's time to get to the working place (this permission is valid till the worker enters the workplace))
4. Worker enters compound (use case 4)
5. Worker uses his/her identity card to obtain protective equipment from the dispenser
6. System identifies the worker and gives out the protective equipment
7. Worker comes 10 minutes before the shift start to its working place and stays there
8. System verifies this by reading workers location
9. The foreman observers the workers during the shift
10. Worker leaves the working place in the 10 minute window following the end of the shift
11. System verifies this by reading workers location
12. Worker uses his/her identity card to exit the hall
13. System identifies the worker and opens the door and signals it is opened
14. Worker is supposed to leave the factory compound by 30 minutes after the shift ends.
15. System verifies this by reading workers location
16. The foreman leaves her/his place 45 minutes after the shift ends

Alternatives and Extensions

Alternative for the step 2:

1. Worker is not at the compound 30 minutes before the shift
2. System notifies the foreman and tells the name of the worker plus provides an estimates how long to get the worker to the compound.
    a) Worker is less than 10 minutes far from the compound (guess by a navigation service)
        i. System notifies the worker to "hurry up"
        ii. System allows the foreman to see the worker's travelling time estimate (access granted for 10 minutes)
            A. Alternative here – the worker is not at the compound after 10 minutes (20 minutes before the shift)
            B. GOTO – 2b (call the replacement)
    b) Worker is more than 10 minutes far from the compound
        i. System notifies the foreman (that the worker is unreachable)
        ii. System notifies the worker that he/she is excluded from the shift
        iii. System selects a replacement worker (with required capabilities) from the stand-by workers and notifies the foreman (name and phone no. of the replacement) and notifies the replacement (place and start of the shift)
        iv. System "remembers" the replacement worker

Alternative for the step 7:

1. Worker is not 10 minutes before the shift start at his/her working place
2. System provides the worker's phone number to the foreman and system grants the foreman to observe the worker's exact location
3. Worker is notified to "hurry up"

Extension to the step 9:

1. A worker does not work satisfactorily or there are issues with production
2. The foreman enters issues to the system

Alternative for the step 10:

1. Worker is after 10 minutes still at his/her working place
2. System notifies the foreman and system grants the foreman to observe the worker's exact location

Alternative for the step 14:

1. Worker is after 30 minutes still at the compound
2. System grants the security to observe the worker's exact location

Subordinate Use Cases Granting the worker access to the building (UC4)

Relation to Requirements The same requirements for KPI sharing across supply chains as in use case UC 4 are reflected in this use case.
The following requirements for factory access control are reflected in the use case:

- R3 – Trust model
- R6 – Privacy awareness among ACS components
- R7 – Role-dependent privacy
- R8 – Location-dependent privacy
- R9 – Enforcing privacy by entity occurrence
- R10 – Entities data sharing schedule
- R11 – Issue/event/process strictly demarcated by time stamps
- R12 – Non-redundancy

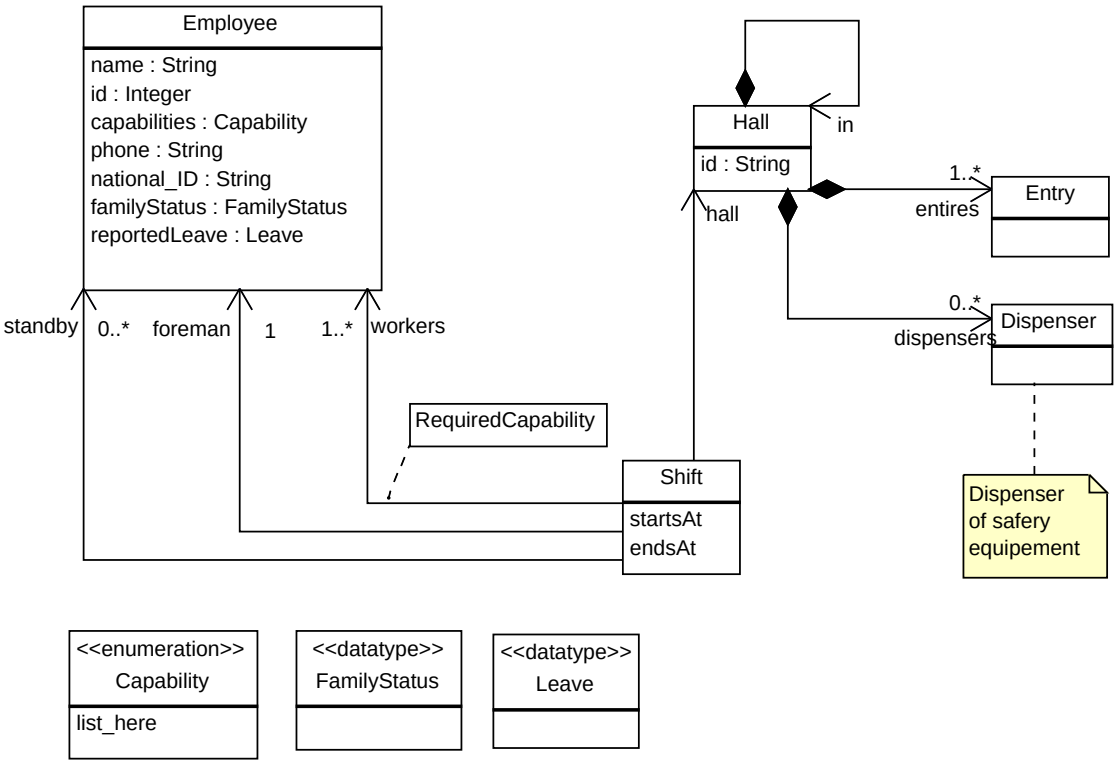

Figure 3.2: Domain model for use-cases

4 State of the Art

During our research we found four main categories of related approaches(Confidentiality Analyses, Access Control, Enforcement, Data Sensitivity).

4.1 Confidentiality Analyses

Under confidentiality analyses we understand to check, whether a system behave according to our privacy [33] rules. One high-level approach for this is Threat Modeling [28]. It checks coarse-grained the system description for security flaws, in our case for privacy. Changes in the system architecture are difficult, because threat modeling uses different models, than architects and developers. In Hoisl et al. [13] the transmissions in service-oriented architecture design is secured. The approach however only checks for integrity and confidentiality, it does not have access control integrated. UMLsec [17] also secures links, in addition it has an access control system integrated. The definition of these access rules are however defined on the control flow, which is more complicated to use than on the dataflow. Dataflow analyses like Joana [27] and code verification approaches such as KeY [1] support the detection of information leaks. Both approaches need the actual source code and are restricted to specific programming languages like Java, which is against our Requirement NFR 2.

4.2 Access Control

The classical access control approaches are DAC [31] and MAC [30]. In both approaches the access right to a file are directly associated with one user. In MAC the file is additionally secured with a passphrase. Because of the direct association to files, no group of users exists. Those groups are described as roles. However, Requirement R2.4 requires access based on the role in one organization. The role based access control RBAC [8] tries to solve this problem. The access rights in RBAC are associated with a role and not directly with the user. This allows to easily give groups of users permission for access. This approach was included for example in SecureUML [20]. Here a modeler specifies roles and permission in an UML class diagram. However, this does not support dynamic access control, based on other contexts, than roles, for example Requirement R2.7 could not be modeled. In the Organization based access control (OrBAC) [18] the context for the access is directly modeled [18]. Because OrBAC does not support the dynamically joining of different entities, the Coalition-OrBAC approach [3] tries to solve this. However, the approach still only supports different entities of the same type. So no joining of completely different entities like an supplier and one manufacturer as

in Requirement R1 is possible. One other approach is Attribute Based Access Control (ARBAC) [15]. Here the access is regulated over different Boolean attributes, which needs to be satisfied, before access to the file can be given. ARBAC does not work on the dataflow and is so far not integrated into an architectural design. In [29], *Thanigaivelan et al.* introduce Context-based Dynamically Reconfigurable Access control (CoDRA). It provides a dynamic configuration and enforcement of policies allowing for static and dynamic constraints. However, it misses design time analysis. In [14], the researchers consider the use of context-aware role-based access control (CARBAC) ontology, which enhances the response time for access rights. The ontologies provide context-aware rule-based privacy control, triple level control (i.e. Resource Description Framework - RDF), and dynamicity in roles. Even though the method supports dynamicity of roles and the results showed only a small overhead, the paper did not describe composition of the rules or how the cooperation between different autonomic actors could be performed.

4.3 Enforcement

After declaring the security policies, these must be enforced. Typically a enforcement platform is used for this. The dynSMAUG framework [19] add this to the ABAC approach. It manages the policies in both outsourcing and provisioning modes, but it is still based on events rather than data flow.

Another enforcement platform is MDSE@R [2]. Here aspect orientated programming allows adding enforcement rules, without changing the original source code. Similarly, [6] targets preventing security attacks by policy-enforcement for dynamic data-flow tracking. More specifically, it uses static analysis for policies and reduces tracking overhead significantly. In other words, it is compiler-based system that work on source level to add new policies without changing the compiler itself. Moreover, a framework [24] captures context and privacy requirements in access control systems. During enforcing the non-conflicted policies, the security requirements also taken into account. In our approach we do not want to concentrate too much on enforcement, but rather reuse existing platforms.

4.4 Data Sensitivity

The privacy and trustworthiness is based on protection of sensitive data. It is crucial to control data disclosure during data storage, process, and sharing. Basically, the start is in identifying the sensitive data and to pick the right presentation of it after applying suitable techniques such as data anonymization or data masking [22].

Anonymization of data as part of trust and privacy preservation is presented in different cases such as [26]. This research addressed data leaks without the need to reveal the sensitive data for data leak detection (DTD) (i.e. could be also detected by policy enforcement). The sensitive data is marked by users and anonymized before sending it to a trusted third party for detection. Nevertheless, it is not clear how the dynamic context could impact the process, which we require in Requirement R1.

Similarly, in clouds, [32] presents an algorithm for anonymization before sharing the data on cloud to prevent data disclosure. It also does not consider the context. Also in [12], data is protected before sending to the cloud, and the decision of anonymization is taken by users instead of developers. Even though the flexible access control here is considered in addition to the trade-off between safety and privacy, requirements such as prediction Requirement R2.1 and performance Requirement NFR1 are not tackled.

The QoCIM framework [21] analyses the data sensitivity, another important research field in Industry 4.0. The framework is based on the quality of the data (Quality-of-Context) analysis. It considers trust, however it is in terms of quality of the meta-data rather then in terms of confidentiality. Also, data sensitivity is designing dynamic security that considers environmental risks [10]. Here, the access control for resources has sensitivity level, time restriction, and groups as security attributes. Nevertheless, it does not consider confidentiality either.

5 Envisioned Approach for Trust Enforcement

The envisioned Trust 4.0 architecture enforces privacy requirements on exchanged information regarding multiple business units working across the entire supply chain. Our suggested architecture builds upon the already presented general architecture for information sharing in distributed supply chains in Figure 2.1. The architecture shown in Figure 5.1 is a concrete instance for supporting the use cases described in Chapter 3. IMA sensors provide information about the physical location of entities and enforce physical access control.

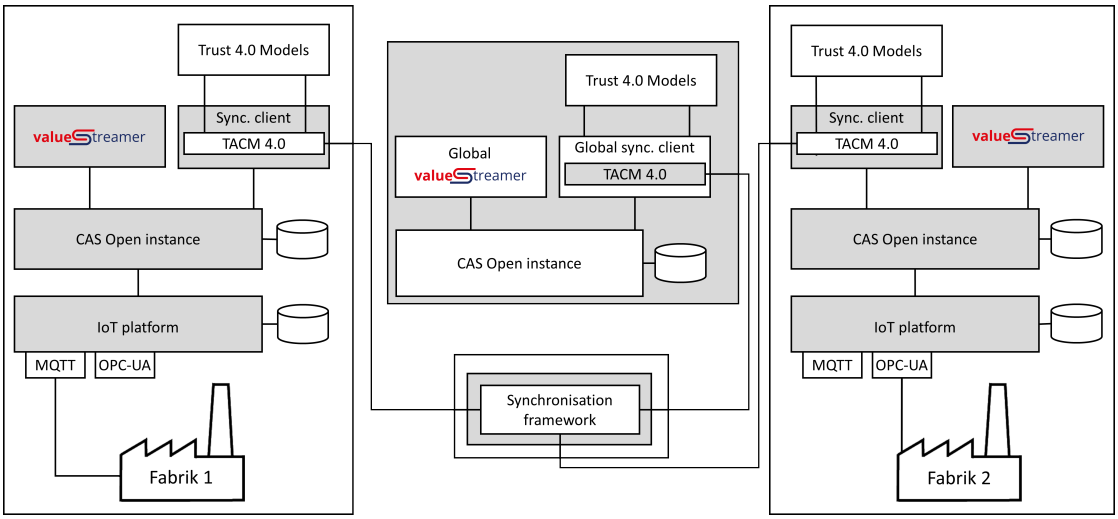

Figure 5.1: Bird's eye view of the Trust 4.0 architecture

The two companies want to share their business data. The data is mostly gathered from different sensors. An IoT platform gathers sensor data with different protocols and stores them in its database. In each company, the data can be accessed with the application server *CAS Open instance*. One example of such an access is the ValueStreamer®. Every time KPIs or other data shall be shared beyond factory borders, the CAS Open server uses its synchronization client. This client then asks its *TACM 4.0* module, which regulates the access control within a company. It therefore analyzes the privacy policies the system's user have modelled, i.e. the *Trust 4.0 Models.* The module contains information about a) the structure of information systems as well as about how information is derived from other information modeled with PCM [23] and a data flow

extension [25], b) the context relevant for the decision such as geographical location of entities or roles of entities, and c) rules for data sharing involving the context information and the shared data formulated in ensembles [4]. The *synchronization client* also manages the synchronisation between the different companies. Therefore it is connected to the *CAS OpenSync* module. This module manages the information exchange between different entities. The synchronisation uses a global *ValueStreamer®* instance with a synchronization client module. The global synchronization client module of the global instance uses the TACM module to determine, whether information can be exchanged or not. Figure 5.1 describes which software components in the different business entities interact across the supply chain:

- ValueStreamer®: lean- and shopfloor-management tool
- CAS Open instance: basic application server for the ValueStreamer®
- Sync. client: manages data sharing between instances as well as mapping and transfer of data objects
- IoT Plattform: manages IoT interfaces and data analytics
- TACM 4.0: connection to the Trust 4.0 Models – PCM and Ensembles; management of privacy issues, i.e., this component asks PCM and Ensemble whether to share an object or not.
- Trust 4.0 Models: PCM and Ensembles governing the access control and data sharing that the TACM 4.0 enforces
- MQTT and OPC UA: IoT protocols used

Figure 5.2 describes the input and output of the Trust 4.0 models in relation with the software components involved in the use cases (see Section 3.2). We will describe Figure 5.2 in the following.

In use case 1, the ValueStreamer® of Factory C queries its synchronization client and the TACM 4.0 component (not shown here, see Figure 5.1) whether to share the KPI quality ration with Factory B. The TACM 4.0 component uses the Trust 4.0 Models to calculate an answer. If the answer is 'no', then no data will be shared. If the answer is 'yes', the data will be shared with Factory B. If Factory B receives the data, the local system will use its local Trust 4.0 Models to calculate, if the data can be given to the responsible foreman.

In use case 2, the same process is executed between Factory B and Factory A on other data. The applied principles remain the same.

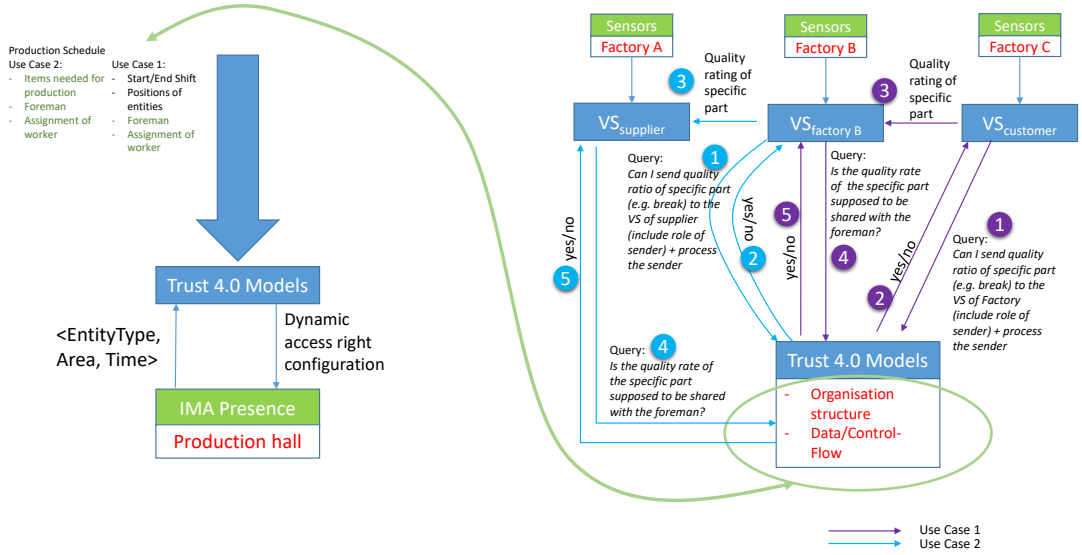

Figure 5.2: Input and output of the Trust 4.0 models

6 Conclusion and Future Work

Industry 4.0 supply chains are the basis of many products and important for the success of numerous companies.

Efficiency is essential in order to be successful in nowadays industrial environments. One way of fostering efficiency is performing global analysis on the distributed supply chain - often by means of exchanging IoT- or KPI-data (Key Performance Indicator). This data can be used by lean- and shopfloor management approaches and tools in order to foster efficiency.

However, globally available information raise trust and privacy concerns. E.g., companies competing often do not want to share business critical information with each other. Thus, trust and privacy-preserving mechanisms are a precondition for data exchange in distributed supply chains. However, this is not easy to achieve: Supply chains in Industry 4.0 are changing rapidly, new stakeholders have to be taken into account and leave again from the supply chain.

Privacy policies might depend on legal frameworks, processes, roles, time and place: privacy policies have to be evaluated in highly dynamic environments and on highly dynamic parameters.

Our goal is to define a reference architecture that allows for privacy-preserving efficiency analysis in distributed Industry 4.0 supply chains.

Our efforts are bases on the analysis of two real world scenarios from industry partners involved in Industry 4.0 supply chains: (a) Lean- and shopfloor management for distributed supply chains and (b) factory access control in Industry 4.0. From these scenarios we have derived requirements and use cases.

We have introduced our use cases in Industry 4.0, concerning privacy and trust modeling. Based on the use cases and requirements, we have searched for existing solutions and found them being laking mostly the dynamic, necessary for the Industry 4.0 domain. Because of this, we introduced a reference architecture and our envisioned approach. Our approach will support the dynamic aspect necessary in Industry 4.0. It will preserve the privacy of each participant.

Due to the early stage of the project, there are still open questions and future work. In the future, we want to provide an in depth view of the combination of PCM and the Ensemble and how they play together to help with dynamic privacy. Here we also want to research, how to update our internal access models with the new state of the environment. In our view, this will be the main work in the future. A possible solution for this could be the integration of iObserve [11], which is combination of runtime and design time analysis.

For further evaluation the approach will be tested in a real Industry 4.0 system. In there all the components of our envisioned approach will be applied.

Without trust - often a result of privacy-preserving mechanisms - data will not be shared along distributed supply chains. Since meaningful data is the precondition for global analysis, efficiency can only be achieved with help from privacy-preserving mechanisms. Our approach of evaluating and enforcing highly dynamic privacy policies in distributed supply chains paves the way for efficient industry 4.0 supply chains.

Bibliography

[1] Wolfgang Ahrendt et al. *Deductive Software Verification – The KeY Book*. Cham: Springer International Publishing, 2016. ISBN: 978-3-319-49811-9 978-3-319-49812-6. (Visited on 02/22/2018).

[2] Mohamed Almorsy, John Grundy, and Amani S. Ibrahim. "Mdse@ r: model-driven security engineering at runtime". In: *Cyberspace Safety and Security*. Springer, 2012, pp. 279–295.

[3] Iman Ben Abdelkrim et al. "Coalition-OrBAC: An Agent-Based Access Control Model for Dynamic Coalitions". In: *Trends and Advances in Information Systems and Technologies*. Ed. by Álvaro Rocha et al. Cham: Springer International Publishing, 2018, pp. 1060–1070. ISBN: 978-3-319-77703-0.

[4] Tomas Bures and et al. "Software Abstractions for Component Interaction in the Internet of Things". In: *Computer* 49.12 (2016), pp. 50–59. ISSN: 0018-9162.

[5] CAS Software AG and Staufen AG. *ValueStreamer*. `http://www.valuestreamer.de/en/home/`. Accessed: 15.03.2018.

[6] Walter Chang, Brandon Streiff, and Calvin Lin. "Efficient and Extensible Security Enforcement Using Dynamic Data Flow Analysis". In: *Proceedings of the 15th ACM Conference on Computer and Communications Security*. CCS '08. Alexandria, Virginia, USA: ACM, 2008, pp. 39–50. ISBN: 978-1-59593-810-7. DOI: `10.1145/1455770.1455778`. URL: `http://doi.acm.org/10.1145/1455770.1455778`.

[7] Alistair Cockburn. *Writing effective use cases*. Addison-Wesley Professional, 2000.

[8] David Ferraiolo, Janet Cugini, and D Richard Kuhn. "Role-based access control (RBAC): Features and motivations". In: *Proceedings of 11th annual computer security application conference*. 1995, pp. 241–48.

[9] OPC Foundation. *OPC Unified Architecture Specification*. "`https://opcfoundation.org/developer-tools/specifications-unified-architecture`". 2008.

[10] M. Fugini, G. Hadjichristofi, and M. Teimourikia. "Dynamic Security Modeling in Risk Management Using Environmental Knowledge". In: *2014 IEEE 23rd International WETICE Conference*. 2014, pp. 429–434. DOI: `10.1109/WETICE.2014.42`.

[11] Robert Heinrich. "Architectural run-time models for performance and privacy analysis in dynamic cloud applications". In: *ACM SIGMETRICS Performance Evaluation Review* 43.4 (2016), pp. 13–22.

[12] Martin Henze et al. “A comprehensive approach to privacy in the cloud-based Internet of Things”. In: *Future Generation Computer Systems* 56 (2016), pp. 701 –718. ISSN: 0167-739X. DOI: https://doi.org/10.1016/j.future.2015.09.016. URL: http://www.sciencedirect.com/science/article/pii/S0167739X15002964.

[13] Bernhard Hoisl, Stefan Sobernig, and Mark Strembeck. “Modeling and enforcing secure object flows in process-driven SOAs: an integrated model-driven approach”. In: *Software & Systems Modeling* 13.2 (2014), pp. 513–548. ISSN: 1619-1366, 1619-1374. (Visited on 02/21/2018).

[14] Shohreh Hosseinzadeh et al. “A Semantic Security Framework and Context-aware Role-based Access Control Ontology for Smart Spaces”. In: *Proceedings of the International Workshop on Semantic Big Data*. SBD ’16. ACM, 2016, 8:1–8:6. ISBN: 978-1-4503-4299-5. DOI: 10.1145/2928294.2928300. URL: http://doi.acm.org/10.1145/2928294.2928300.

[15] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo. “Attribute-Based Access Control”. In: *Computer* 48.2 (Feb. 2015), pp. 85–88. ISSN: 0018-9162. DOI: 10.1109/MC.2015.33.

[16] ISO/IEC. *ISO/IEC 20922:2016 Information technology – Message Queuing Telemetry Transport (MQTT) v3.1.1.* ”https://www.iso.org/standard/69466.html”. 2016.

[17] Jan Jürjens. “UMLsec: Extending UML for secure systems development”. In: *UML’02*. Springer, 2002, pp. 412–425.

[18] A. A. E. Kalam et al. “Organization based access control”. In: *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks*. June 2003, pp. 120–131. DOI: 10.1109/POLICY.2003.1206966.

[19] R. Laborde et al. “dynSMAUG: A dynamic security management framework driven by situations”. In: *Proceedings of CSNet’17*. Oct. 2017, pp. 1–8.

[20] Torsten Lodderstedt, David Basin, and Jürgen Doser. “SecureUML: A UML-based modeling language for model-driven security”. In: *UML’02*. Springer, 2002, pp. 426–441.

[21] Pierrick Marie et al. “The QoCIM Framework: Concepts and Tools for Quality of Context Management”. In: *Context in Computing: A Cross-Disciplinary Approach for Modeling the Real World*. Ed. by Patrick Brézillon and Avelino J. Gonzalez. New York, NY: Springer New York, 2014, pp. 155–172. ISBN: 978-1-4939-1887-4.

[22] Balaji Raghunathan. *The Complete Book of Data Anonymization: From Planning to Implementation*. Boston, MA, USA: Auerbach Publications, 2013. ISBN: 1439877300, 9781439877302.

[23] Ralf Reussner and et al. *Modeling and simulating software architectures: the Palladio approach*. Cambridge, Massachusetts: MIT Press, Oct. 2016. 377 pp. ISBN: 978-0-262-03476-0.

[24] A. Samuel et al. “A Framework for Composition and Enforcement of Privacy-Aware and Context-Driven Authorization Mechanism for Multimedia Big Data”. In: *IEEE Transactions on Multimedia* 17.9 (2015), pp. 1484–1494. ISSN: 1520-9210. DOI: 10.1109/TMM.2015.2458299.

[25] Stephan Seifermann. “Architectural Data Flow Analysis”. In: *13th Working IEEE/IFIP Conference on Software Architecture (WICSA16)*. Venice, Italy: IEEE, Apr. 2016, pp. 270–271. DOI: 10.1109/WICSA.2016.49.

[26] X. Shu, D. Yao, and E. Bertino. “Privacy-Preserving Detection of Sensitive Data Exposure”. In: *IEEE Transactions on Information Forensics and Security* 10.5 (2015), pp. 1092–1103. ISSN: 1556-6013. DOI: 10.1109/TIFS.2015.2398363.

[27] Gregor Snelting et al. “Checking probabilistic noninterference using JOANA”. In: *it-Information Technology* 56.6 (2014), pp. 280–287.

[28] Frank Swiderski and Window Snyder. *Threat Modeling*. Redmond, WA, USA: Microsoft Press, 2004. ISBN: 978-0-7356-1991-3.

[29] Nanda Kumar Thanigaivelan et al. “CoDRA: Context-based dynamically reconfigurable access control system for android”. In: *Journal of Network and Computer Applications* 101 (2018), pp. 1–17.

[30] Sabrina De Capitani di Vimercati and Pierangela Samarati. “Mandatory Access Control Policy (MAC)”. In: *Encyclopedia of Cryptography and Security*. Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 758–758. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_822. URL: https://doi.org/10.1007/978-1-4419-5906-5_822.

[31] Sabrina De Capitani di Vimercati. “Discretionary Access Control Policies (DAC)”. In: *Encyclopedia of Cryptography and Security*. Ed. by Henk C. A. van Tilborg and Sushil Jajodia. Boston, MA: Springer US, 2011, pp. 356–358. ISBN: 978-1-4419-5906-5. DOI: 10.1007/978-1-4419-5906-5_817. URL: https://doi.org/10.1007/978-1-4419-5906-5_817.

[32] J. Wang et al. “Providing privacy preserving in Cloud computing”. In: *3rd International Conference on Human System Interaction*. 2010, pp. 472–475. DOI: 10.1109/HSI.2010.5514526.

[33] Alan F Westin. “Privacy and freedom, atheneum”. In: *New York* 7 (1967).