# TOWARDS A COLLABORATIVE ACCES CONTROL MODEL FOR PI: A FIRST EXPLORATION OF THE NEEDS AND REQUIREMENTS


| | |
|---|---|
| Catherine Cassan | Mobilise, VUB |
| Shiqi Sun | Mobilise, VUB |
| Philippe Michiels | Imec |
| Cathy Macharis | Mobilise, VUB |

**Abstract**

The concept of Physical Internet (PI) assumes an extensive data-sharing between entities partaking in the network to realise its potential of an optimised logistics network. While the advantages of this concept are clearly shown in theory, the practical implementation gives rise to some objections. The logistics sector is very competitive, and the sharing of data requires a high level of trust between entities. A level of trust that is hard to gain in dynamic, ad-hoc collaborations. In the context of Industry 4.0, where similar challenge arise, potential schemes for data access control are already developed. Our paper aims to evaluate which requirements should be met to make an access control scheme applicable in PI and if any of the existing schemes fits these requirements. We found that, although each access control scheme offers interesting perspectives, no single one can fulfil all requirements. We therefore conclude that a specific access control model should be developed for PI.

## 1. Introduction

The Physical Internet (PI) (Montreuil et al., 2010) theorem includes a view of the logistics ecosystem as a service-oriented, highly dynamic environment with a high level of data sharing between different (competing) companies. Digitalisation and service-orientation are trends that can already be observed in logistics research today, demonstrating clear potential for increasing the sustainability of logistics. However, real-life applications are only limited and further development of techniques and technology on the one hand and related business models on the other hand is needed (Pan et al., 2019).

One of the challenges to be addressed is the data-security issue, as information needs to be accessible to all who need it, but needs to be protected from unauthorised views at the same time. In traditional information systems, a provider needed only to deal with a known set of users (e.g. the employees), generally divided into a coarse-grained set of roles ("user", "admin", "guest",…). This system can easily be closed of from the 'outside world' by traditional protection systems such as firewalls. For a dynamic, service oriented architecture however, this is fare from adequate as dynamic access to specific pieces of information needs to be granted to specific users. In short, a more flexible and open way to share and protect is needed. To the best of our knowledge, no specific research has addressed this topic in a PI context (Yuan & Tong, 2005).

Access control models are a common way to address this topic and has widly been studied in the field of computer siences. Following the definention of Mohamed et al. (2022), an access control model "defines the enforcement of the authorization model to decide whether to allow or deny access for a subject to a protected recourse", with 'authorization model' defined as "the model for the definition of access rights" and 'subject' as "the active entity to which access rights are granted". It allows access to specific data based on a set of specific rules and policies that can be adapted to the specific situation. Many access control models have been developed over the years, from very simple list-based systems, to complex, hybrid metamodels. In the remainder of this paper we will discuss the most common basic models.

Recently this topic has also been researched in the context of Industry 4.0 (B Leander, 2020, among others). Industry 4.0 was a phrase coined by the German government at the Hanover fair in 2011. Waidner & Kasper (2016) summarize it as (1) horizontal integration through value networks (2) end-to-end digital integration of engineering across the entire value chain and (3) vertical integration and networked manufacturing systems. This definition shows a close relation to PI, where the aspects of horizontal integration, end-to-end planning and tracking and vertical integration of the logistics network are also key aspects. The research into data access control in the context of Logistics 4.0 can therefore be considered as an interesting basis for PI access control schemes.

In this paper, we will first describe the most commonly referred to access control schemes in literature and describe the requirements set for a Industry 4.0 acces control model. Next, we will describe the setting of the PI application developed in the Physical Internet Living Lab (PILL) project. From this

setting, we will use a thougthexperiment to discover what specific requirements should be met for an access control model to be suitable for PI. Finally we will discuss which elements of the existing access control models are relevant to PI and draw conclusions for further research.

## 2. Potential Acces Control models

In computer siences, the topic of access control is widly studied and many different access control models were proposed. Yuan & Tong (2005) found three access control models most commonly used in a context of web service security and described a fourth, alternative model:

- Identity Based Access Control (IBAC) (Lampson, B.W, 1969): in this model, access control is directly associated with a specific subject. Access Control Lists (ACL) are a common example of this model. Although simple in concept, this model quickly becomes hard to menage if a large number of subjects and/or permissions is involved;
- Role Based Access Control (RBAC) (Sandhu et al. 1996): in this model, subjects are assigned to roles, who are then given specific permissions. This offers a significant simplification compared to IBAC, as it allows to manage the user-role and role-permission sets indipendantly and grouped. However, this approach still remains rather static and in more complex systems can lead to an explosion of the number of roles, in extreme cases creating more roles then subjects.
- Latice based access control (LBAC) (Sandhu, R.S., 1993): in this model permissions are assigned based on a lattice of security labels on the one hand and categories on the other. Subjects are then assigned to a a cell and receive the associated permissions, much like in a RBAC model, but with the benefit of having two dimensions to assing subjects to. Again, this approach remains rather static and added complexity will lead to an explotion of the number of cells necessary.
- Atribute based access control (ABAC) (Yuan & Tong, 2005): in this model, subjects, resources and environments each are assigned a set of attributes. Attributes of a subject can include a role, but not necessarily. Access is then granted by checking a set of rules allowing a subject with attributes X and Y to access a resource with attributes A and B under circumstances corresponding to an environment E.

In more recent work, Leander et al. (2021) confirm the relevance of RBAC and ABAC for Industry 4.0 applications. They also refer to Task Based Access Control as a potential interesting alternative.

- Task Based Access Control (Thomas & Sandhu, 1998): this model is based on a set of authorization-task-units wherein for each specific function (task) a set of necessary approvals and dependencys is defined. Once the task is completed, the authorization becomes invalid.

## 3. Setting

Within the PILL project we focused on the route finding stage of a transport, i.e. the development of a routing algorithm and a booking logic. A 'route' in this context is considered to the entire trip from origin to destination of a container, including temporary storage, transhipment etc, if necessary. Once the container is (un)stuffed, we assume the start of a new route.
In the following paragraphs we will first define which actors are involved in this process. Next, we will elaborate on the different steps that were identified in the process. Finally, we will shortly describe the two routingalgorithms that were developed in the process and how they integrate the different steps to find feasible routes.

### 3.1 Business roles

Within the PILL project, the term 'entities' is used for the legal entities responsible for different parts of the logistic chain (Cassan C. et al., 2022). These are the overarching decision-makers who set the main goals of the companies and negotiate the general business agreements in relation with other entities. Any one entity is considered to have multiple possible business roles within the PI-ecosystem. Although widly used, no clear definition of 'business role' was found in literature. For the purpose of this research, we define it as a coherent set of actions, responsibilities and permissions, logically carried out by a single decision-making unit to performe a well defined step in the execution of a task. Note that this definition can be applied at different levels of abstraction. For our purpose, we focus on a high level view, considering the main steps in transport as actions and the entities as decision-making units.
The definition of each entity as a combination of different business roles allows for a clear definition of each role, while still allowing for the multiple combinations of roles each real-life entity may incorporate. As no previously defined roles for logistics where found in literature, we defined the relevant roles to be considered within the project, through analysis of the current processes and discussions with the advisory board members. The following roles where considered to be relevant within the PI-ecosystem, when considering the route-finding and booking process:

- The Transporter role is responsible for the actual movements of goods. They organise the actual transport and are in charge of the schedules and routes of individual movers
- The Node operator role is responsible for the operations within a PI-node. They have one or more fixed locations and handle the transfer of goods from one mover to an other. They can also store containers during their route and serve as a depot for empty containers after the route is completed.
- The Cargo owner (shipper or consignee) is the party currently responsible for the cargo (either sending or receiving, depending on the Incoterm). They set the constrains and preferences for a route (e.g. where and when cargo should be picked-up or delivered, the relative importance of cost, sustainability, speed,…).

- The Expeditor role is responsible for the planning of the route cargo takes. The select a series of transporters and nodes to fulfil this route, based on the constraints and preferences set by the cargo owner.
- The Asset owner: is the entity that owns the specific assets. For simplicity reasons, we did not consider asset owners for movers within PILL. Assets which are leased or chartered are considered to be owned by the transporter. Only container owners are considered as separate entities, as they define the return location of empty containers, which is relevant for the routing.

Additionally, policy roles (responsible for governing the physical network and rules applied to the physical cargo) and governance roles (responsible for governing the digital network and rules applied to data) where defined. As they are less relevant to the current discussion, they are not elaborated on here.

### 3.2 Steps in planning a route

While defining the PI-prototype in the PILL project, several distinct stages in the process of planning a container route were defined. Each of them represents a distinct set of tasks necessary to find a suitable route. However, depending on the approach taken, some can happen simultaneously.

- Step 1: Network discovery:
  In this stage of the process, the aim is to build a representation of the (relevant) logistics network. Entities in the PI network aim to find information about their neighbours and share their own information;
- Step 2: Routefinding:
  In this stage, an expeditor searches for (an) optimal route(s) for a specific shipment, depending on the relevant priorities and constraints set by the cargo owner;
- Step 3: Capacity checks:
  This stage consists of checking if there is capacity available with each of the entities involved in the optimal route(s);
- Step 4: Booking:
  In this stage, the actual booking is made. All entities involved confirm that they will perform the requested tasks an under what conditions;
- Step 5: Transport:
  In the final stage, the shipment is actually transported. This stage will in itself consist of several more stages, but as the PILL project focusses on stage 1 to 4, no further distinction is made at this time.

### 3.3 Potential approaches

Within the PILL project, two potential approaches to fulfil the above steps were researched. As it is yet to be determined which one offers the best solution, both will be described shortly.

The Communication Based PI Routing (CPIR) algorithm (Sun et al., n.d.) stays very close to the Digital Internet (DI) concept of routing through routers and assumes knowledge of the network at any individual node is limited to the existence of connected nodes . No additional information about these neighbouring nodes is stored locally. Routing request are send from an origin node (backtracking from the destination node is also possible, but will be ignored in this text for simplicity) to all known nodes, who then check the (future) availability of movers at their location who have the capacity to fullfill the route before closing time. If the route is incomplete at this point, the neighbouring nodes of the origin node will send on the routing request to their neighbours and so on, until a complete route is formed. The complete routes are then reported back to the origin node where the preferred route is selected (manually or automatically) and the tasks necessary to complete the route are booked with the appropriate entities.

In the Physical Internet application of A* (PIA*) all entities in the network share their capabilities openly (Cassan C. et al., 2022). In the PILL project 'capabilities' can be understood as the ability of the entity to fullfill a specific task within a logistic operation (e.g. 'transport', 'store', '(de)compose',…). Consequently, every node is capable of making a local copy of the (relevant part of the) network. This local copies of the network are updated automatically whenever an entity enters or leaves the network, adds additional nodes or makes changes to their capabilities and can keep track of additional information such as road saturation, low watertables etc. This dynamic overview of the network is defined as the 'network state'. Based on the network state, feasible routes can initially be calculated locally at the origin (or destination) node and ordened according to the users preferences. Only after the initial routingfinding step is completed, the other entities involved in the preferred route are contacted to check for available capacity. If no capacity is available for the prefered route, the second preferred route is checked for capacity and so on, until a full route can be booked.

## 4. Thought experiment

### 4.1 Step 1: Network discovery

In this step, a relevant view of the network is constructed. As locations and capabilities are considered public information, no specific access rules are relevant for this discovery. All members of the network can get full access, given their identity as a PI entity is confirmed. The information they need to share themselves depends on their business roles: a transporter should share their transport modes, schedules etc, a node operator their location, capabilities and opening hours and so on. By defining the roles beforehand, a strict definition of the minimal information to be shared can be obtained, making sure all relevant information is available for the next steps.

### 4.2 Step 2: Routefinding

In the PIA* routing scheme, no interaction with other entities is done at this stage. The expeditor uses the local copy of the network constructed in the previous step to find feasible routes.
In the CPIR routing scheme, the routing request is first send to all neighbouring nodes. The node then sends on the necessary information to the available transporters at their site. The first determent to decide who to send the information to at this stage is therefore the business role. Specifically, the roles of 'node' and 'transporter' are relevant at this stage. They determine (1) who to send information to and (2) what information to include. However, this information alone is not enough. It is theoretically possible to send all requests to all nodes, but this would 1) take up computing time for irrelevant computations and 2) would violate the 'need-to-know' principle. If all nodes and all tranpsorters where to receive all requests, they would gain far more knowledge about the flows in the network then they need to perform their tasks.
So, in addition to the business role, information about the relation of the node/transporter to the requesting expeditor/node is needed. This information can not be universaly defined (as is the case for business roles) but needs to be specified for each node. Additionally, this information might change over time with the addition or deletion of new nodes or transports. Therefore, to define who would receive this information, an access system is needed that relates to the current network state and is flexible over time.
For the node-to-node communication, this information would be an equivalent of 'has a direct connection to me'. Nodes unable to handle the requested containertype will simply reply 'no' to the request. Nodes located in the wrong direction will return a route that is longer and/or more expensive then alternative nodes in the right direction, resulting in the routingprocess to be aborted for these nodes.
For the node-to-transporter communication, this information would be an equivalent of 'linked to me' for trains or barges and an equivalent of 'is located neer me' or 'already has a visit planned' for trucks. Transporters who don't have a visit during the available time window for the delivery will simply reply 'no' to the request.

### 4.3 Step 3: Capacity check

In the CPIR routing scheme, the capacity check is done simultaneously to the routefinding: only routes for which there is capacity available are returned to the requesting expeditor.
In the PIA* routing scheme, routefinding is done locally, so no capacity information is available yet. An additional step to confirm capacity is needed. To do this, the requesting expeditor will send a capacity request to the relevant transporters and node operators in their optimal route(s). In this case, the fact that an entity has the business role of 'transporter' or 'node operator' clearly becomes insufficient. Also adding information on the current network state (defining 'who is connected to me'), as was done for the routefinding, will not suffice in this case.

The key information needed to know who to send the request to becomes 'takes part in this route' rather than the business role of the entity or their connections to the requesting node. This information is highly dynamic and will change for each individual route requested. Still, the business role of an actor remains relevant: depending on whether this actor is a transporter, node operator or asset owner, different information about the route needs to be shared. For example, for a container owner the total duration of the trip will be relevant, but the exact route information is not needed. On the contrary, for a transporter, only the earliest/latest pickup and dropoff is relevant, and the exact location of the pickup and dropoff nodes are crucial.

### 4.4 Step 4: Booking

In this stage the selection of the route is formalized and all entities involved sign of on their respective tasks within the route. The information exchanged in this stage consists of signatures, payementdetails etc. This falls outside of the scope of this paper and will therefore not be discussed here.

### 4.5 Step 5: Transport

Within the PILL project, we have not yet explored the communications during transport, as we focussed on the routefinding and booking step. However, it stands to reason that during transport, information needs to be shared between the actors partaking in the transport (e.g. events tracking, disruptionallersts, optimisation opportunities,…). Like for the capacity check, only knowing either the business role, geographical location or their connection to the specific transport will not be enough to determine who to send what information. A combination of all three pieces of information will be needed to share sufficient, but need-to-know information.

## 5. Discussion

PI promises to create a more efficient logistics system. One of the key aspects to achieve this, is a more automated data sharing and processing between independent (possibly competing) logistic actors. As trust between those actors might be limited, a system needs to be in place that assures that the information shared is both sufficient and strictly on need-to-know basis. In current day logistics, routeplanning and capacity checks are (mainly) done by email or telephone contacts. In these human-to-human interactions, the amount of information shared is based on the common sence or intuition of the humans involved. However, in machine-to-machine communication a set of rules needs to be defined to achieve this goal.

From our thought-experiment, we can derive that we need an access control model that can take into account:

- The business role of the entities;
- The position of the entity in the network relative to the requesting node;
- The current step in the routeplanning (i.e. booking, routefinding,…);

- The selection of the entity to perform a specific task in a route;
- The exact location and next task(s) to be performed (during the transport step).

It is clear that a simple IBAC based model will not be able to handle the vast number of entities represented in the network and their dynamic interactions. Even if each entity would keep a list of the relevant entities to contact in the routefinding step, it is imposible to keep track of each individual request or transport in this way.

RBAC gives the advantage of already making a distinction between the different business roles entities can have. Although the business roles are relevant to the access control, and should therefore be taken into account in the access model for PI, RBAC itself is shown to be to static to fullfill the PI access control needs. Indeed, it is the business role of an entity relative to the current shipment that needs to be taken into account, not the business role(s) an entity has as such.

LBAC has similar issues as RBAC in this context: the second dimention in this model gives the advantage of adding additional criteria but doesn't answer give an answer to the need to adapt access control for each individual shipment.

ABAC partly solves this issue by adding the 'environment' as an aspect to take into account when sharing data. Business roles, geographical location and other relevant aspects could be included as different attributes of an entity as well. However, the concept of 'environment' in ABAC remains still relatively static: the stages of a transport process could be defined here (i.e. routefinding, capacity check, booking, in transport,…) defining which information needs to be shared in which stage. However, the individual connection of which entity is performing a specific business role within the context of a specific shipment is still lacking.

TBAC is the only access control model evaluated that offers the potential to link specific rights to an entity only in the context of a specific shipment at a specific stage. However, as the concept was never fully developed, the potential of this solution remains unclear.

## 6. Conclusion

We can conclude that, though several existing access control model offer interesting elements to be incorporated into an adequate access control model for PI, no ideal solution could be found in the reviewed literature. This finding confirms the conclusion of Tolone et al. (2005), who evaluated access control models for collaborative systems in a more general context, and refines it to the context of PI. Although this conclusion cannot be considered recent (dating from 2005), more recent findings confirm that despite the amount of access control model proposed, transition to practice is currently still limited because of the lack of maturity of these models and their inability to meet all requirements for a true collaborative access control model (Paci et al., 2018).

## 7. Limitations and further research

This research represents a first step in defining the requirements for datasharing in a PI context. Further research remains necessary to test the aptness and completeness of these requirements in different settings.

## References


Cassan C.; Finck J.; Lemos V.; Michiels P.; Sun S.; Van Bever, & D. (2022). *D1.6.1 midway report;* PILL | imec (imec-int.com)

Lampson, B.W. (1969). *Dynamic Protection Structures*. *35*, 27–38. https://doi.org/10.1145/1478559.1478563

Leander, B. (2020). Access Control Models to secure Industry 4.0 Industrial Automation and Control Systems. *Es.Mdh.Se*. https://www.es.mdh.se/pdf_publications/6088.pdf

Leander, Bjorn, Causevic, A., Hansson, H., & Lindstrom, T. (2021). Toward an Ideal Access Control Strategy for Industry 4.0 Manufacturing Systems. *IEEE Access*, *9*, 114037–114050. https://doi.org/10.1109/ACCESS.2021.3104649

Mohamed, A. K. Y. S., Auer, D., Hofer, D., & Küng, J. (2022). A systematic literature review for authorization and access control: definitions, strategies and models. *International Journal of Web Information Systems*, *18*(2–3), 156–180. https://doi.org/10.1108/IJWIS-04-2022-0077

Montreuil, B., Meller, R. D., & Ballot, E. (2010). Towards a Physical Internet: the impact on logistics facilities and material handling systems design and innovation. *Progress in Material Handling Research*, 305–327.

Paci, F., Squicciarini, A., & Zannone, N. (2018). Survey on access control for community-centered collaborative systems. *ACM Computing Surveys*, *51*(1). https://doi.org/10.1145/3146025

Pan, S., Zhong, R. Y., & Qu, T. (2019). Smart product-service systems in interoperable logistics: Design and implementation prospects. *Advanced Engineering Informatics*, *42*(October), 100996. https://doi.org/10.1016/j.aei.2019.100996

Sandhu, R.S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *Computer*, *29*(2), 38–47. https://doi.org/10.1109/2.485845

Sandhu, Ravi S. (1993). Lattice-Based Acces Control Models. *Computer*, *26*(11), 9–19. https://doi.org/10.1109/2.241422.

Sun, S., Cassan, C., & Macharis, C. (n.d.). Communication is Computation : a Privacy-Protecting Routing Algorithm for Physical Internet. *Unpublished Manuscript*.

Thomas, R. K., & Sandhu, R. S. (1998). *Task-based authorization controls (TBAC): a family of models*

*for active and enterprise-oriented authorization management*. *May 2015*, 166–181. https://doi.org/10.1007/978-0-387-35285-5_10

Tolone, W., Ahn, G. J., Pai, T., & Hong, S. P. (2005). Access control in collaborative systems. *ACM Computing Surveys*, *37*(1), 29–41. https://doi.org/10.1145/1057977.1057979

Waidner, M., & Kasper, M. (2016). Security in industrie 4.0 - Challenges and solutions for the fourth industrial revolution. *Proceedings of the 2016 Design, Automation and Test in Europe Conference and Exhibition, DATE 2016*, 1303–1308. https://doi.org/10.3850/9783981537079_1005

Yuan, E., & Tong, J. (2005). Attributed Based Access Control (ABAC) for web services. *Proceedings - 2005 IEEE International Conference on Web Services, ICWS 2005*, *2005*, 561–569. https://doi.org/10.1109/ICWS.2005.25