in: Proceedings of ACM
Conference on Computer Supported Cooperative Work
(CSCW 2002), ACM-Press, New York , S. 196 - 205

# A New Dimension in Access Control: Studying Maintenance Engineering across Organizational Boundaries

**Gunnar Stevens**[1] **and Volker Wulf**[1,2]

[1]Institute for Information Systems
University of Siegen
Hölderlinstr. 3, 57068 Siegen, Germany
[stevens/wulf]@fb5.uni-siegen.de

[2]Fraunhofer Institute for Applied Information Technology (FhG-FIT)
Schloß Birlinghoven, St. Augustin, Germany
wulf@fit.fraunhofer.de

## ABSTRACT

Inter-organizational cooperation has specific requirements for access control. The paper presents the results from a field study which looks at the cooperation between two engineering offices and a steel mill.  Based on these findings we have developed new mechanisms for access control in groupware. These mechanisms allow to restrict operations on shared data while or even after they take place. The new access mechanisms can be decomposed and implemented into a component-based framework. We show how this framework can be extended to realize additional mechanisms for access control with little efforts.

### Keywords

inter-organizational cooperation, case study, access control, tailorability

## INTRODUCTION

Inter-organizational cooperation can be seen as a generic term for a large spectrum of joint activities crossing organizational boundaries. Interestingly it has not yet attracted much attention within the CSCW community (for exceptions see: [1], [2]; [8]).

However inter-organizational cooperation has been since long time investigated within the business administration community. Harms paraphrase the main conflict in inter-organizational cooperation as follows: *"The interests of the individual organizations coincide as far as they concern the cooperative tasks, whereas in other areas interest may be contradictory or in the best of cases do not touch"* [11]. It is interesting to investigate empirically whether such a clear distinction between areas of common and contradictory interests exists.

Looking from a CSCW perspective to inter-organizational cooperation, it requires coupling on the side of the work-processes with an integration on the side of the computer applications. Thereby conflicts between economic autonomy and information coupling may emerge due to the interrelation of mutual and contradictory interests.

To open internal information sources for external access is a far reaching but often desirable support for inter-organizational cooperation. Due to the existence of contradictory interests, access of external cooperation partners has to be controlled in an appropriate manner. Therefore it is worth investigating whether the existing approaches to access control offer appropriate mechanisms to support inter-organizational cooperation without violating the individual partners' interests.

In the following we investigate the state of the art in access control for groupware. To understand the specifics of inter-organizational cooperation in detail, we look at a case study from the field of maintenance engineering. A steel mill wants to open its electronic drawing archives to external service providers. The findings of this case study result in new requirements for the design of access control. An implementation of these requirements will be shown and discussed.

## ACCESS CONTROL

The design of appropriate mechanisms for access control was from the beginning an important topic in the CSCW discussion. Greif and Sarin [7] and Ellis, Gibb and Rein [6] argue that traditional approaches do not allow to specify access control strategies adequately.

Among the traditional approaches the access model developed by Lampson [13] was extremely influential and widely spread. He distinguishes three dimensions for specifying access rights: subjects, objects and operations. Seen from a user-oriented point of view, an access control strategy specified which subjects are allowed to carry out a certain operation on a specific object. The subject dimension was typically defined by a list of all users. The object dimension consists of a list of individual files. With regard to operations, one could choose between "*read*" and "*write*".

The work by Shen and Dewan [16, 4] mark a major step in overcoming the limitations of traditional approaches. They allow for a more fine-grained specification of access rights

*CSCW'02*, November 16–20, 2002, New Orleans, Louisiana, USA.

on the object- and operation-dimensions. Access can be specified even for individual elements within a file (e.g. a sentence within a text file). Access can also be specified with regard to a big variety of groupware-related operations (e.g. copying). To cope with the higher efforts necessary to define more fine-grained access rights, Shen and Dewan [16] have implemented a hierarchical order on each of the three dimensions (e.g. a user can take a role or belong to a group; the "*InsertR*"-operation belongs to the group of WriteR-operations). Access rights get inherited along the lines of the hierarchical order (e.g. all members inherit the group's access rights). To express exceptions from the inheritance rules, Shen and Dewan allow specifying negative access rights explicitly. Sikkel [17] and Wulf et al. [24] stay with the main premises of Shen and Dewan's access model. However they modify the inheritance mechanisms to ease the specification of access control strategies.

So CSCW research in area of access control extended Lampson's basic approach by differentiating the objects-, subjects-, and operations- dimensions. However, it did not challenge one of Lampson's basic assumptions: that one wants to and is able to determine the access permissions ex ante (before the actual access takes place).

This assumption has been challenged by work on optimistic access control strategies in the field of Information Systems. Optimistic security policies, as described by Povey [14], are based on the following idea: "*Legitimate and optimistic access control takes the approach of assuming that most accesses will rely* on controls external to the system *to ensure that the organization's security policy is maintained. ... In an optimistic system, enforcement of the security policy is retrospective, and relies on administrators to detect unreasonable access and takes steps to compensate for the action. Such steps might include: undoing illegitimate modifications, taking punitive action (e.g. firing, or prosecuting individuals) or removing privileges*"

Povey's approach is based on five preconditions, which will not to be examined more closely here. The differences compared to the traditional mechanisms of access control, which he called pessimistic, are shown in table 1.

Dewan and Shen [5] have distinguished between pessimistic and optimistic control strategies. They call a strategy optimistic if users are allowed to modify protected data locally even if they cannot be stored globally later on. The following draws on Povey's [14,15] understanding of optimistic control strategies.

| ATTRIBUTE | PESSIMISTIC | OPTIMISTIC |
|---|---|---|
| Access Decision | Prospective | Retrospective |
| Access Enforcement | Deny | Recover/Deter |
| Cost of Violation | None | Some |
| Flexibility | None | Some |

**Table 1:** Pessimistic vs. optimistic access control strategies (cf. [15])

With regard to access control in groupware, we see three gaps which have not yet been tackled sufficiently:

*Empirical gap*: Interestingly there are very few case studies which investigate access control in real world settings. Even in the CSCW-community most of the access control models are developed without empirical grounding (for exceptions see: [18]; [3]; [21]). To our knowledge there is not any empirical study which looks at requirements for access control in inter-organizational cooperation.

*Theoretical gap:* Pessimistic approaches to access control require ex-antes specification of the permissions. Optimistic approaches offer the chance to define the access policy ex-post. However, there does not exist a general model which classifies access policies according to the time-spot in which the decision about the legitimacy of an attempt to access data is taken.

*Flexibility gap:* The access models developed within the CSCW-community offer more flexibility than Lampson's model in specifying access rights. However, these models can not be extended during run-time. While the access permissions can be changed, the dimensions specifying the access rights stay stable.

In the following, we will present work which tackles the three gaps. First, we will investigate requirements for access control derived from a case study dealing with inter-organizational cooperation.

## CASE STUDY

We have investigated the maintenance engineering processes of a major German steel mill in the Ruhr area over a period of three years. The investigations took place in the context of the ORGTECH project (see [25]). A goal was to improve the inter-organizational cooperation between two engineering offices and the steel mill. The engineering offices are located 15 and 25 kilometers from the steel mill. They take on sub contractual work for the steel mill in the field of maintenance engineering, e.g. the construction and documentation of steel furnace components. A construction department inside the steel mill coordinates the planning, construction and documentation processes, and manages the contacts with external offices at the steel mill.

### Research methodology

The OrgTech project follows an action research approach: the Integrated Organization and Technology Development (OTD) framework (see [23]). The OTD process is characterized by a simultaneous development of the workplace, organizational and technical systems; the management of (existing) conflicts by discursive means, and the participation of the organization members affected. During the course of the project, it turned out that external access to the steel mill's electronic archives became a crucial bottleneck. The results presented in this paper come from a variety of different sources:

- Analysis of the work situation: The field of application was examined by means of more than 25 semi-structured interviews, workplace observations, and further questioning about special problem areas.
- Analysis of the documents available: The relevant artifacts were investigated by looking at the given documents especially the drawings and system descriptions.
- System evaluation: The given archives systems were examined by means of a usability evaluation, especially with regard to task adequacy.
- Project workshops: During various workshops with members of the three organizations, organizational and technological interventions were discussed to improve the maintenance engineering process.

### Process of Plant Maintenance: An Overview

In the following we will look at the schematically depicted processes of maintenance engineering (cf. figure 1). The Maintenance Engineering Department of the steel mill deals with repairing and improving the plant. Maintenance engineering is a distributed process, in which different organizational units of the steel mill and of the external engineering offices are involved.

In general, the starting point for a maintenance order is the plant operator. The steel mill consists of several organizationally independent plants, e.g. coke chambers, blast-furnance. The operators of each plant control the production equipment and machinery in their plant. When maintenance is necessary, the maintenance department of the plant operator asks the internal construction department for further processing. Depending on the type of order and the measures required, the transaction is handled internally or passed on to an external engineering office. An extern order will be prepared and surveyed by the responsible contact person in the internal construction department. For this reason, the necessary drawings and documents are compiled from the archives and passed on to the engineering office for further processing. Usually, the order specifications contain errors and need further clarification right from the very beginning. So discussions among the different actors and extensive re-ordering of drawings often become necessary. New drawings and documents have to be found, coordination work has to be done and contacts with other departments have to be initiated.

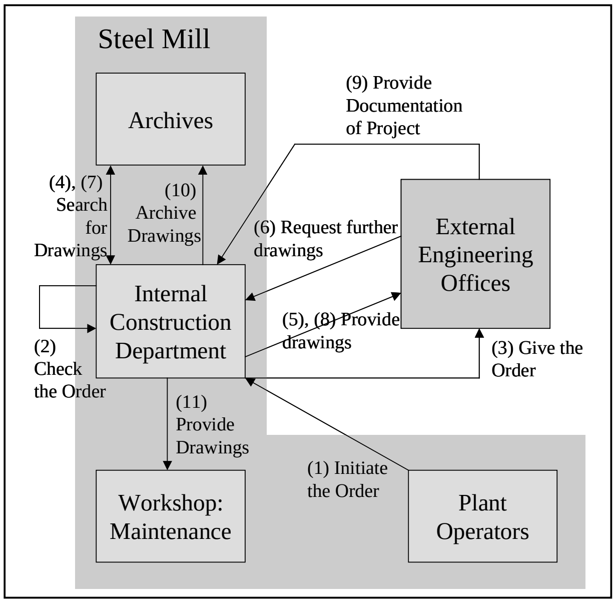

Steel Mill
Archives
(9) Provide Documentation of Project
(4), (7) Search for Drawings
(10) Archive Drawings
(6) Request further drawings
External Engineering Offices
Internal Construction Department
(5), (8) Provide drawings
(2) Check the Order
(3) Give the Order
(11) Provide Drawings
(1) Initiate the Order
Workshop: Maintenance
Plant Operators

**Figure 1:** Process of Maintenance Engineering

After an external office finishes its engineering task, the internal construction department has to check it, include the modified and new drawings into the archives and initiate the production process of the required spare parts. After being either produced by the internal workshop or ordered externally, the spare parts are assembled into the plant. While this is the general process schema of maintenance engineering, various sorts of informal communication and self-organized variations of the process can be found.

In the early phases of the project, the external engineering offices complained about insufficient task specification on the side of MeltIt and lacking electronic exchange of drawings between them and the steel mill. They suggested to open the electronic drawing archives of MeltIt to ease cooperation. Whereas the attitude of MeltIt towards an external access to the archives was quite ambivalent. The attitude of the internal engineers could be described with the words: *The external service provider should be able to work independently but MeltIt has to keep the control.*

So we had to investigate options for an external access to the archives more closely.

### Work Practice: Pattern of External Access

With regard to the external engineers' access to the archives, we have to distinguish between the process prescribed by the steel mill's formal organization and the actual work practice.

The division of labor prescribed by the formal organization of the steel mill may roughly be characterized as follows: The internal engineer in charge of handling a certain project finds all necessary drawings for the external service provider and passes them over to him. The external engineer works with the drawings, revises them when necessary, and returns them later on to the steel mill. When the documentation of a project arrives in the mill, it undergoes a quality control by the internal engineer. An engineer of the steel mill describes the situation as follows: *"The external service provider normally receives the whole documentation, sometimes also the general idea how to solve the problem. After this first clarification they remain executing organ. In the end of the project we have to do the content and geographical as well as the structural inspection."*

In such an ideal case there is no need for an external access to the archives. In practice it often happens, though, that additional drawing are requested continuously during the whole engineering process. This is done in several ways. The drawings are ordered either by phone, fax, or e-mail. A specific fax form had been created by one of the offices for ordering drawings. These requests are typically directed to the internal engineer responsible for the project. She typically checks the request, comments it and passes it to the archives group. They search for the drawings and put them into a specific shelf in the archives. From this shelf the drawings are picked up later. Because it takes quite a bit of a drive to the steel mill, colleagues who have to go to the mill anyway are often asked to pick up the drawings.

However it is often not easy to specify the required drawings exactly without having access to the archives. So the external engineers often drive to the mill and search together with an employee of the archives group or by themselves in the drawing archives.

The internal engineers often try to limit their efforts to the absolutely necessary when passing over the documents. However, formally it is part of their task, to decide whether a drawing should be handed over to an external engineering office. The dilemma for the internal construction department may be depicted as follows: If an external service provider contacts the archives directly, the internal construction department has less work. However if problems arise, the internal department has the responsibility without being sufficiently involved. In certain cases they even loose control in the end of a project. Occasionally external office delivers the drawing directly to the archives without involving the construction department. In this case they may not even get aware of the fact that something has been changed.

### Inter-Organizational Relationship: Between Competition and Cooperation

More than ten years ago, MeltIt had started to outsource an increasing amount of work in maintenance engineering. A MeltIt employee described it this way *"The number of employees has decreased continuously during the last years. [...] At the moment there is a sort of stagnation at a low level with increasing outsourcing"*.

The outsourcing process has let to an increased uncertainty among MeltIt's maintenance engineers whose department was partly replaced by external service providers. The outsourcing process has also changed the function of the internal construction department. Regarding the external offices, it takes different roles, which are partly conflicting. Especially the roles of the administrator of the orders, of the competing participant in the market, and of the security guard have to be mentioned here. In this sense, the internal construction department sees the extern engineering offices not only as contractors, but also as a competing market participant. As the engineering offices work also for competing steel mills, in some cases they may even be seen as potential spies. This constellation results in the imponderability of the relation.

Also at another level there is one more competitive element in the relationship between the steel mill and its external service providers. The engineering offices are not only working for MeltIt but also for its regional and global competitors. As the competition is very fierce on the world market of steel, small technological innovations may lead to important competitive advantages.  There is an unwritten rule that external service would not pass technological innovations from one client to another. However, the remaining risk increases if the external service providers can access the database in an unrestricted way.

External engineering offices and the steel mill also compete for human resources. During the runtime of the ORGTECH-Project, the steel mill hired an engineer from one of the external engineering offices without asking for approval before hand. As payment and social benefits are higher in the steel mill than in most of its service providers, it is often attractive for employees of the external offices to change sides. However, the leave of their best employees, creates major problems and anger for the bosses of the external offices.

So there always exist identical as well as diverging interests between the internals and the external engineering organization. In this matter our observation differs from Harm [11] who assumes that the inter-organizational cooperation is divided into cooperating and competing tasks. As we will show, the coexistence of cooperation and competition influences the design of the tools to access the electronic drawing archives.

### Conclusions from the case study

The business goals and the work processes determine what the critical assets of an organizational unit are. Matters in the inter-organizational cooperation which touch these assets, are judged to be more critically than those which are rather at the borderline. At MeltIt it is the archives, and the access to them, which represents a competitive advantage for the internal construction department. If the inter-organizational cooperation refers to this area, this may lead to special tensions.

By introducing tele-cooperation systems, previous control mechanisms could vanish. This results into tension becoming virulent and may even inhibit the introduction of computer systems. Sydow et al.  [22, p. 219] describes such a case from the insurance industry where independent broker were not given access to IT systems rather for competitive than for technical reasons. In order to prevent this to happen, IT systems for inter-organizational cooperation have to take this tension into consideration.

| Dimension | Specification | Description |
|---|---|---|
| Subject | External service provider | Who wants to have access to a drawing? |
| Object | Content | Drawings themselves or descriptions of drawing (metadata such as drawing-number, base-number)? |
| | State of processing | Is the drawing in work? |
| Operation | Type of access | Reading, writing, or modifying drawings or descriptions of drawings (metadata)? |
| Situation | Order | With regard to which order is access required? |
| | Time | Do the external engineers still work on the corresponding order? |
| | Priority of the order | Which priority does the order have? |

**Table 2:** Relevant dimensions for specifying external access to the steel mill's archives

So it is important to study the current mechanisms of access control more in detail. To tackle the theoretical gap, we want to propose an extended model of access control.

## EXTENDED MECHANISMS FOR ACCESS CONTROL

As a result of the field study, table 2 gives a survey on the dimensions which an internal engineer takes into account when deciding whether to grant access to external engineers. The first three dimensions are basically case-specific incarnations of the dimensions that Lampson [13] had already worked out. The fourth dimension "*situation*" relates the access to drawings or to descriptions of drawings to the order given to the external service provider. This dimension is rather typical for inter-organizational cooperation in case cooperation is based on individual projects.

Looking at the way external engineering offices get access to the drawing archives, there is an interesting aspect which attracts attention. The steel mill specifies access rights for external service providers only partly ex-ante. The formally prescribed process consists of a mixture of ex-ante specification and an on-going negotiation and exploration of access rights.

Access permissions are provided at the beginning of the project for those drawings which are handed over to the external engineering offices. However, these drawings are typically not sufficient (cf. section 3). Therefore, different electronic media, like telephone, fax machines, and e-mail are applied to negotiate access rights at the moment they are required. However, the lacking integration of theses media with the archives database requires double efforts to input the inquiry. Moreover, the external engineer can not explore the content of the database. This is, however, strongly required because the classification scheme of the database is not applied consistently (cf. [12]). Finally, the drawings are not delivered electronically to the external offices, which results in considerable time delay between query specification and check of results.

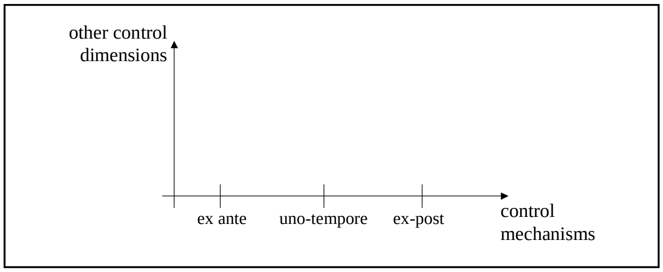


**Figure 2:** Control mechanisms a new dimension in access control

Due to these problems a couple of informal work practices have emerged which let the external service provider search in the archives' database in an unrestricted way. These practices take an optimistic stance towards access control. However, they contain different mechanisms which make the external access perceivable for internal actors. First, the terminal from which the external engineers can access the archives database is located within the archives department. So searching as well as printing is carried out "*under the eyes*" of the archives' workers. Moreover, when leaving the mill, the external engineers have to pass a guard at the gate, who may get suspicious in case too many drawings are taken out.

While these formal and informal practices seems to be appropriate in the current situation, they do not offer any protection if the external offices can access the electronic archives from their home offices. Therefore, it is worth to discuss how to extend the given approaches in order to enable comparable practices in the future. A theoretical framework is helpful to generalize the experiences beyond the given case study.

In order to classify mechanisms for access control, we will refer to the point in time, at which the access permissions are defined. There are three points in time to be distinguished:

- There is an **ex-ante** control if the permissions have been defined before the access.
- There is an **uno-tempore** control if the permissions are defined at the moment of the access.

- There is an **ex-post** control if the permissions are checked after the access took place.

The traditional approaches to access control belong to the category of ex-ante mechanisms. An example of uno-tempore control can be found when the external engineers sent a fax to their internal counterpart and ask for a specific set of drawings. An example of an ex-post control mechanism is the peripheral surveillance of the external search activities by the archives' workers. Ex-post mechanisms are only applicable if use and misuse become visible, and misuse can be sanctioned.

Stiemerling and Wulf [21] have empirically investigated access control mechanisms within organizations of the administrative sector. Three cases studies were given which could be interpreted according to the framework provided here. In two cases, trusted third persons acted as gate keepers to the data of other users. Whenever the owner of the data was not available and an unexpected access requirement emerged, the gate keepers could be asked to allow access. In these cases an uno-tempore approach compensated for problems resulting from ex-ante specification. The third case described, how access to documents in an open letter boxes was controlled by mutual awareness. Colleagues passing by the letter boxes could observe at least in principle who dealt with whose documents in which way. So the social control realized an ex-post control mechanism.

The work of Stiemerling and Wulf is also interesting because it reveals that different access control mechanisms can be applied in a combined manner. So an access control system should be implemented which provides different control mechanisms and which allows to combine these mechanisms flexibly.

These considerations lead us to tackle the flexibility gap. We need to build an access control system whose different dimension can be adapted flexibly.

## ADOS-X: A COMPONENT-BASED IMPLEMENTATION OF EXTENDED ACCESS CONTROL MECHANISMS

We built an application which allows the external engineering offices to access the electronic drawing archives of the steel mill. It is called ADOS-X because the database which contains the electronic archives is named ADOS. In describing ADOS-X, special focus will be given to the mechanisms for access control.

In order to be able to tailor the access control strategy while running the program, the application is built of software components (so-called FLEXIBEANS), which can be (re-) assembled during runtime by the users (cf. [19, 20]).

At this point the question arises, who the relevant users are. We assumed that the application should allow the internal engineering department to define their own access policy towards the external service providers. Due to the ambivalence in their relationship, the new system should not reduce the external offices' dependency from the internal construction department. This would be, for instance, the case if the access policy would be defined by the steel mill's IT department. Such a system would probably not be accepted by the internal engineers. So the decomposition of the application into components should be comprehensible for the internal engineers.

As the research on component based tailorability is quite new, there is not yet any method for such a decomposition. Therefore we referred to results from the field of object-oriented software development. The WAM-approach by Züllighoven [26] is a method, which claims to keep the semantic gap between users and developers small. By assuming that an application consists out of tools, automates, and materials, an application is decomposed into objects which are meaningful to users.

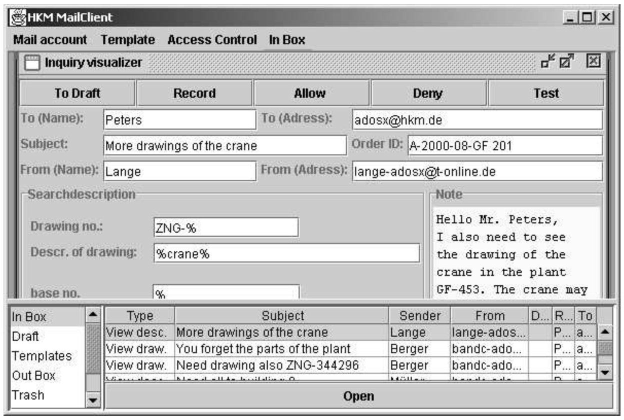
The WAM approach was also applied to build support for cooperative work (cf. [9]). A mail box metaphor was developed to decompose a workflow application. Our application, ADOS-X, is based on this metaphor, but extends it in the way that the users have the option to automate certain aspects of the document flow. By a special component, called sorter, the user is able to decide whether an inquiry to the database should be handled automatically. Due to the mail box metaphor, ADOS-X looks like an e-mail program at the user interface (cf. figure 3).

### Technical Implementation

The FLEXIBEAN model, developed by Stiemerling (see [20]) is an extension of the JavaBean model (cf. [10]). The model allows the recomposition of components during runtime.

Within the FLEXIBEAN model there are two types of components: basic and abstract components. Basic components are written in Java. They form the basic modules for assembly. Abstract components are built from other components. They consist of a number of components and their connections. Once defined, abstract components can be used to build abstract components of a higher level. This feature allows building hierarchical structures. The ADOS-X component presented in figure 4 is an example of an abstract component.

There are two types of interfaces for the exchange of data between components: *events* and *shared objects*. Events



To (Name): Peters
To (Adress): adosx@hkm.de
Subject: More drawings of the crane
Order ID: A-2000-08-GF 201
From (Name): Lange
From (Adress): lange-adosx@t-online.de

Drawing no.: ZNG-%
Descr. of drawing: %crane%
base no. %

Hello Mr. Peters,
I also need to see
the drawing of the
crane in the plant
GF-453. The crane may

| Type | Subject | Sender | From | D... | R... | To |
|---|---|---|---|---|---|---|
| View desc. | More drawings of the crane | Lange | lange-ados... |  | P... | a... |
| View draw. | You forget the parts of the plant | Berger | bandc-ado... |  | P... | a... |
| View draw. | Need drawing also ZNG-344296 | Berger | bandc-ado... |  | P... | a... |

**Figure 3:** ADOS-X client of the internal engineer

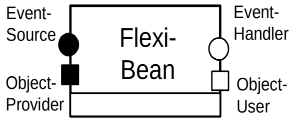
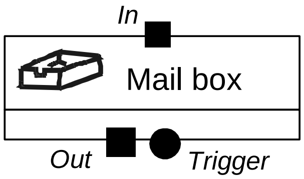
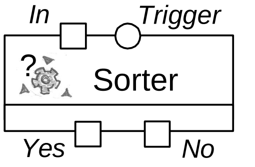
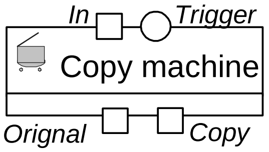
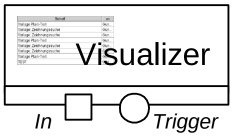
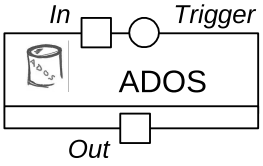
| Component | Description |
|---|---|
|  Event-<br>Source<br>Flexi-<br>Bean<br>Event-<br>Handler<br>Object-<br>Provider<br>Object-<br>User | **FLEXIBEAN**<br>The circles and boxes are ports, through which the components interact with each other. An instance of a component can be named individually to ease users' understanding. |
|  | **Mail box**<br>The mail box is the residence for documents. Documents may be put in via the "*in*"-port or taken out via the "*out*"-port. If the state of the mail box changes, an event is sent via the "*trigger*"-port.<br>The "*see*"-port allows introspection via a *visualizer*-component. |
|  | **Sorter**<br>The sorter component has one entrance and two exits, which can be linked to a mail box. According to the setting of the sorter, a document is transported from the "*in*"-port to the "*yes*"-port or to the "*no*"-port. It is activated via the "*trigger*"-port.<br>The sorter represents the classical access control system. In the current system version only some of the dimensions presented in table 2 are realized (e.g. sender, receiver, basic number). |
|  | **Copy machine**<br>The copy machine has one entrance and two exits, which can be linked to mail boxes. The incoming message is transported from the "*in*"-port into the "*original*"-port. A copy is made and transported to the "*copy*"-port. The copy machine is activated via the "*trigger*"-entrance. |
|  | **Visualizer**<br>The visualizer allows to view the content of a mail box. The visualizer is activated via the "*trigger*"-port. The mail box is connected via the "*in*"-port. |
|  | **ADOS**<br>The ADOS-component provides the connection with the database. The mail box containing the query is connected to the "*in*"-port. The component transmits the query to the database, receives the search results and transfers them to the "*out*"-port. The component is activated via the "*trigger*"-port. |

**Table 3:** Basic components of ADOS-X

allow components to transmit state changes to other components (push-mechanism). Shared objects provide components the option to investigate the state of another component (pull-mechanism). When visualizing components in this paper (e.g. table 3), we mark the event-sources with a filled circle, the event-receiver with an empty circle. The provider of a shared object is marked with a filled square, the recipient of a shared object with an empty square. The interfaces of the components are named and typed. Only interfaces of the same type but with contrary polarity can be connected.

The components define a program which may be performed in a specified tailoring environment: the Evolve-platform. The Evolve-platform allows to add or delete components during runtime. Moreover, the connections between the components can be changed during runtime.

### User Scenarios for ADOS-X

The ADOS-X application, tailored for the needs of the internal engineers, is shown in figure 3. It was built from the basic components shown in table 3. For sake of simplicity, in table 3 we left out some of the components which implement aspects of the visualization.

Some of the access control mechanisms mentioned above have been realized within this version of the application. Other mechanisms can be implemented by adding components or transforming the connections between them.

In the following we will show how ADOS-X can be tailored by adjusting sorter-components. If a user wants to adjust a

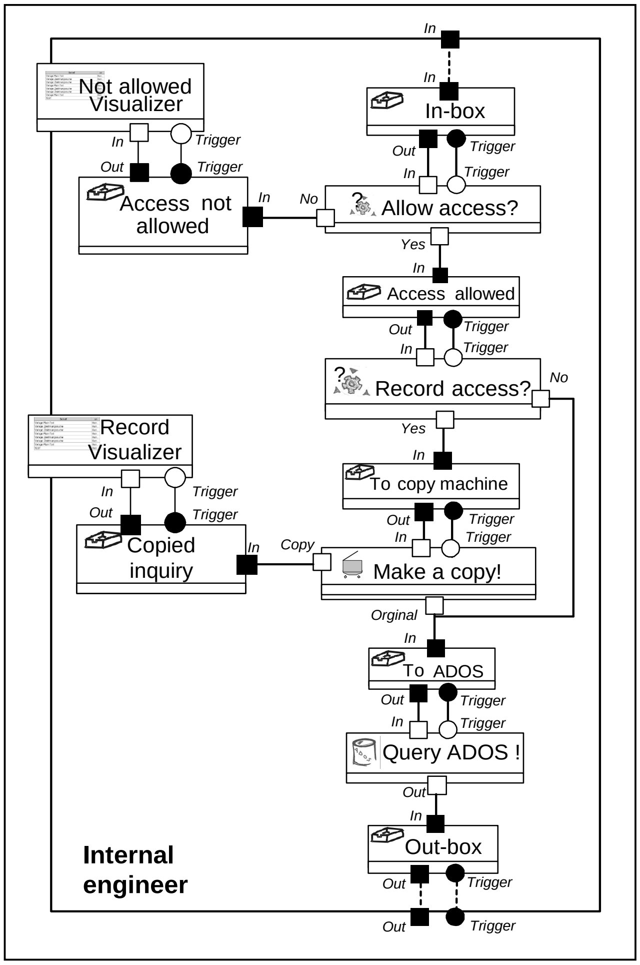
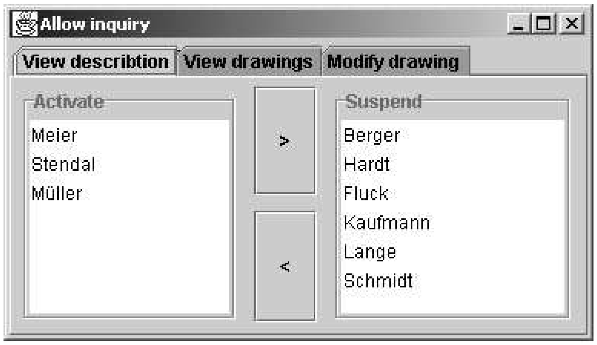


**Figure 4:** Tailorable composition of components to realize access control

sorter, he first selects the persons to grant access. The access is generally denied until it is permitted. Figure 5 shows how the access to read metadata can be granted (operation "*view descriptions*"). By clicking the „<"-button, a user can be moved to the list of those who have permission to view the describing attributes concerning a specific drawing (metadata). Such a permission can be revoked by selecting a user and pushing the ">"-button. The following scenarios are realizable by tailoring the sorter-components.


Allow inquiry

View describtion | View drawings | Modify drawing

Activate
Meier
Stendal
Müller

>
<

Suspend
Berger
Hardt
Fluck
Kaufmann
Lange
Schmidt

**Figure 5:** A sorter's tailoring options

In the actual version of the application, the tailoring options are limited to choices on two control- dimensions: subjects and operations. Access rights for the following operations can be specified: view the description specifying a drawing (metadata), view the drawing, and modify the drawing (and its description). Figure 5 shows a screenshot of an interface which offers these tailoring options.

*First Case: "Access is manually authorized"*

ADOS-X can be tailored in a way that any query of the external engineers need to be authorized manually. For this purpose the "*Allow-Access?*"-sorter has to be tailored in a way that it moves the incoming documents to the "*no*"-exit. This means, that all queries end up in the mail box "*Access not allowed*". The internal engineer can now view these queries via the "*Not allowed*"-visualizer. The visualizer offers options for a manual treatment of the query such as forwarding it to ADOS, editing it, or sending it back to the external engineers. These options are not represented in figure 4.

This option requires a manual authorization of any attempt to access ADOS. It represents an uno-tempore control mechanism. As it corresponds to the actual practice, we have chosen it to be the ADOS-X standard configuration.

*Second Case "Access is allowed but electronically recorded"*

The internal engineers can tailor the system that carries out all queries automatically, but records them. In this case the "*Record access?*"-sorter must be configured in a way that it moves the queries to the "*yes*"-exit. Queries will take the way via the "*copy-machine*"-component ("*Make a copy!*"). This component copies the query and moves the copies via the "*copy*"-exit to the mail box "*Copied inquiry*". A visualizer allows the internal engineers to check the queries later on. The original query is moved via the "*original*"-exit to the mail box "*To ADOS*". Then the "*ADOS"*-component ("*Query ADOS!*") processes the query and forwards the search results to the mail box "*Out-box"*. From this mail box they are sent via E-mail to the external engineering office which posted the query.

As the queries of the external engineers are recorded, they are available for a subsequent check by the internal engineers. So this mechanism represents an ex-post control mechanism.

*Third Case: "Access is allowed"*

The deviation via the "*copy-machine*"-component ("*Make a copy!"*) may be cut short by adjusting the "*Record access?*"-sorter for documents accordingly. Via the "*no*"-*exit*, queries of certain engineers are now sent directly to the "*Query-ADOS*"-component. Such a configuration of ADOS-X realizes a classical ex-ante control mechanism, because the access permissions are specified before the access takes place.

The arrangement of components presented in figure 4 allows to realize a variety of access mechanisms by tailoring the sorters. To tackle the flexibility gap, we demonstrate how to meet new requirements for access control by means of abstract components, modified compositions, and new basic components.

### Abstract Components, Modified Compositions, and New Components: More Flexibility

During our work with the steel mill some actors, especially from the management, were concerned that engineers would be able to specify their access policy in a completely decentralized and autonomous manner. To deal with these concerns, our approach allows to support the role of an administrator responsible for the overall security.

Our concept of abstract components proved to be very helpful to satisfy these requirements. The composition of basic components presented in figure 4 can be turned into an abstract component. A name for the abstract component can be chosen (e.g. "*internal engineer*"-component). Moreover, one has to declare which ports of the internal components should be visible to the outside of the abstract component. In our case the "*in*"-port of the mail box "*In-box*" and the "*trigger*"- and "*out*"-port of the mail box "*Out-box*"- became the ports for the abstract component "*internal engineer*" (cf. figure 5). These ports could be even renamed to make the behavior of the abstract component better understandable to the users.

The new composition is shown in figure 6. Each internal engineer defines access by means of his specific instance of an "*internal engineer*" component. But instead of sending all search results directly to the external engineering offices, the data gets collected by a sorter which sends it to the "*security admin*" abstract component. This abstract component can be built as an instance of the "*internal engineer*"-component. However, the "ADOS"-component should be removed to avoid querying the database twice. The "*security admin*" abstract component can be tailored to realize the organization's over all security standards (e.g. record all queries).

During our work with the steel mill another requirement for access control came up. Most of the actors were not too worried if external engineering offices got access to individual drawings. However, they feared that someone could take out the documentation of whole plants or big parts of them. To deal with this concern, we thought of programming a new basic component which would count and restrict the amount of drawings sent to a specific engineering office. The internal engineers could tailor this component by specifying an amount of drawings per time unit. This new component could be integrated into the "*internal engineer*" abstract component (between the "*ADOS*"-component and the "*out-box*"-mail box). In this way the internal engineers or the administrator gained additional flexibility in specifying their access policy.

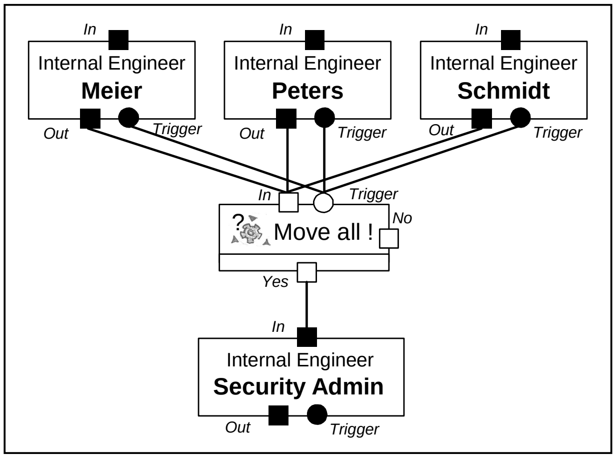


**Figure 6:** Access control by involving a security administrator

## CONCLUSION

Newer concepts in management science like organizational networks, outsourcing, or virtual organizations are based on intense inter-organizational cooperation. However, inter-organizational cooperation has not yet attracted much attention within the CSCW community. We have presented a case study of inter-organizational cooperation from the steel industry. Analyzing the relationship between the external and the internal engineering department, the co-presence of cooperation and competition turned out to exist. Though joint projects required a tight coupling across organizational boundaries, competition stayed in place.

We have investigated new concepts of access control, to allow sharing of material stored in electronic repositories of one of the partners. Traditional access control only allows to choose between the "*allowed*" and "*forbidden*" options. Such an approach implies the assumption that it is possible to distinguish between the "*allowed*" and "*forbidden*" options *ex-ante*. It was shown that this approach does not comply with the organizational requirements. Therefore, a new dimension in the design of access control was conceptualized. Mechanisms of *uno-tempore* and *ex-post* access control have been developed which offer new options to deal with the coexistence of cooperation and competition. However, such mechanisms may be also relevant for other settings of cooperative work (cf. [21]).

Looking at the implementation, we have chosen a component-based framework which allows to tailor the applications even at runtime. ADOS-X supports the actual practice of decentralized access control. Nevertheless, we hope that it is designed flexibly enough to avoid becoming an obstacle when changes in the cooperation arise. It should support processes of organizational development by "*soft*" technical transitions. However, ADOS-X still has to undergo this prove of concept.

## REFERENCES

1. Bowers. J., Button, G. and Sharrock, W.: Workflow from within and without: Technology and cooperation in the print industry shopfloor, in: Proceedings of ECSCW'95, Kluwer, Dordrecht, 1995, pp. 51-66.

2. Cohen, A. L., Cash, D. and Muller, M.: Designing to support adversarial collaboration, in: Proceedings of the ACM Conference on Computer Supported

Cooperative Work (CSCW 2000); ACM Press, New York, 2000, pp. 31-39.

3. Coulouris, G., Dollimore J. and Roberts M.: Secure communication in non-uniform trust environments; vorgelegt bei: ECOOP Workshop on Distributed Object Security, Brussels, 1998.
4. Dewan, P. and Shen, H.: Flexible Meta Access-Control for Collaborative Applications; in: Proceedings of the ACM Conference on Computer Supported Cooperative Work (CSCW-98), Seattle, 1998, pp. 247-256.
5. Dewan, P and Shen, H.: Controlling Access in Multiuser Interfaces; in: ACM Transaction on Comuter-Human Interaction; Vol. 5, No. 1, 1998, pp. 34-62.
6. Ellis, C. A., Gibbs, S. J. and Rein, G. L.: Groupware - some Issues and Experiences; in: Communications of the ACM, Vol. 34, No. 1, 1991, pp. 38-58.
7. Greif, I. and Sarin, S.: Data Sharing in group work; in: Proceedings of the First Conference on Computer-Supported Cooperative Work; ACM Press; New York; 1986, pp. 175-183.
8. Grinter, R. : Recomposition: Putting it all back together again, in: Proceedings of CSCW' 98, ACM Press, New York, 1989, pp. 393-402.
9. Gryczan G.: Prozeßmuster zur Unterstützung kooperativer Tätigkeit; Deutscher Universitätsverlag, Wiesbaden, 1996.
10. Hamilton, G.: JavaBean Version 1.01; Sun Microsystems; 1997.
11. Harms, V.: Interessenlagen und Interessenkonflikte bei der zwischenbetrieblichen Kooperation; Würzburg, Physica-Verlag, 1973.
12. Hinrichs, J.: Telecooperation in Engineering Offices - The problem of archiving. in: Designing Cooperative Systems (COOP 2000), IOS Press, Amsterdam, 2000, pp. 259-274.
13. Lampson, B.: Protection, in: ACM Operation Systems Review, Vol. 8, 1974, pp. 18-24.
14. Povey, D.: Optimistic Security: A new access control paradigm; in: Proceedings of the 1999 New Security Paradigms Workshop, 1999.
15. Povey, D.: Optimistic Security: A new access control paradigm. Panel Presentation: Highlights of the 1999 New Security Paradigms Workshop. National Information Systems Security Conference (NISSC), Arlington, Virginia, 1999.
16. Shen, H and Dewan, P.: Access Control for Collaborative Environments; in: Proceedings of the Conference on Computer-Supported Cooperative Work (CSCW92), ACM Press, New York, 1992, pp. 51-58.
17. Sikkel, K.: A Group-based Authorization Model for Computer-Supported Cooperative Work; Arbeitspapiere der GMD 1055, GMD, Sankt Augustin, 1997.
18. Sikkel K. and Stiemerling O.: User-Oriented Authorization in Collaborative Environments; in Proceedings of COOP '98, 26.-29.5.98, Cannes, 1998, pp. 175-183.
19. Stiemerling, O.: FlexiBeans Specification V 2.0; Arbeitspapier, Unsiversität Bonn, Informatik III, 1998.
20. Stiemerling, O, Hinken, R. and Cremers, A. B.: The EVOLVE Tailoring Platform: Supporting the Evolution of Component-Based Groupware; in: Proceedings of EDOC'99, IEEE Press, Mannheim, Sept. 27.-30., 1999, pp. 106-115.
21. Stiemerling, O., Wulf, V.: Beyond 'Yes or No' - Extending Access Control in Groupware with Awareness and Negotiation; Group Decision and Negotiation; Vol. 9, 2000, pp. 221-235.
22. Sydow, J., Windeler, A., Krebs, M., Loose, A. and Well, B.: Organisation von Netwerken : Strukturationstheoretische Analysen der Vermittlungspraxis in Versicherungsnetzwerken; Westdeutscher Verlag, Opladen, 1995.
23. Wulf, V. and Rohde, M.: Towards an Integrated Organization and Technology Development; in: Proceedings of the Symposium on Designing Interactive Systems, 23. - 25.8.1995, Ann Arbor (Michigan), ACM-Press, New York, 1995, pp. 55-64.
24. Wulf, V., Stiemerling, O. and Pfeifer, A.: Tailoring Groupware for Different Scopes of Validity, in: Behaviour & Information Technology, Vol. 18, No. 3, 1999, pp. 199-212.
25. Wulf, V., Krings, M.,Stiemerling, O., Iacucci G., Maidhof, M., Peters, R., Fuchs-Fronhofen, P., Nett, B. and Hinrichs, J.: Improving Inter-Organizational Processes with Integrated Organization and Technology Development, in: JUCS, Vol. 5, Issue 6, 1999, pp. 339-365
26. Züllighoven H.: Das objektorientierte Konstruktionshandbuch nach dem Werkzeug & Material-Ansatz; dpunkt-Verlag, Heidelberg, 1998.