INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN, ICED'09
24 - 27 AUGUST 2009, STANFORD UNIVERSITY, STANFORD, CA, USA

DEVELOPMENT OF SECURE COLLABORATION MODELS IN PRODUCT LIFECYCLE MANAGEMENET

Wei Liu[1, 2], Min Wang[1], Da Yong Zhang[1] and Yong Zeng[1]
(1) Concordia University, Canada (2) Northwestern Polytechnical University, China

ABSTRACT
This paper formalizes product lifecycle management (PLM) based on axiomatic theory of design modeling. Collaboration and secure collaboration issues in PLM are of major concern. Representation models of collaboration mechanism in the listed collaboration scenarios are proposed. Secure collaboration scenario is highlighted and possible solutions are modeled to refine the mathematical model of product lifecycle management. Respective available mechanisms are discussed.

Keywords: Axiomatic Theory of Design Modeling; Product Lifecycle Management; Collaboration; Security

1. INTRODUCTION
Product Lifecycle Management (PLM) is a systematic concept for the integrated management of all the product related information and processes across the extended enterprise throughout the entire product lifecycle, ranging from design, to production, distribution, maintenance, and retirement [1]. With the adoption of PLM, enterprises can gain many benefits including mass customization, quicker delivery, higher quality, minimized manufacturing costs, reduced project failure rates, increased and quick innovation, higher plant uptimes, effective management and use of corporate intellectual capital, effective communication among different groups at dispersed locations, less industrial and commercial waste throughout every phase of the product life cycle, and more environmentally awareness [2-6]. Among many issues in PLM, such as information management, process management and application integration [7], this paper addresses intraorganizational and interorganizational secure collaboration. Collaboration is characterized by information sharing whereas information security requires the protection of sensitive information.
In a collaborative product development environment, different partners, such as planner, designer, manufacturer, and supplier, can share the common data and communicate with each other through conference tools, such as email, instant messaging tools etc. Some efforts have been made by researchers to support real-time collaborative design and analysis tasks for product development. For example, Sun [8] proposed a development process model on integrated modeling and simulation environment, and event-driven constraint-triggered decision pushed model to depict product design process. Other literature is devoted to establish the framework of collaboration. For example, Gruat La Forme [9] proposed a collaboration characterization model in supply chains, focusing on information exchanged between partners as well as on the exploitation of this sharing.
In the same time, security issue is of paramount importance for product lifecycle management. Several security properties are required in a PLM system, such as confidentiality, integrity, availability, and access control. There are some widely used security protocols, such as SSL/TLS, PKI, Kerberos, and IPSec, that can be used to enforce these security properties of PLM. With regard to access control, some useful models have been proposed. For example, Leong et al. proposed a mixed access control model for a workspace-oriented distributed product data management (DPDM) system [10]. Cera et al. [11, 12] and Kim et al. [13] developed a new technique, role-based viewing, for collaborative 3D assembly design. Wang et al. proposed an access control model, S-RBDDAC, for collaborative design data [14].
As mentioned above, researchers gain more insights into secure collaboration approaches in PLM. However, contributions to the secure collaboration scenarios have only been evaluated to a limited extent. An investigation into the models for various collaboration scenarios and secure collaboration scenarios in the PLM is beneficial to analyze, validate and use the existing secure collaboration

approaches, even lead to novel ones. This paper aims to develop such secure collaboration models for the PLM. A formal representation for the PLM as the prerequisite for analysis of various scenarios and as a meta-model for secure collaboration models is proposed in Section 2. In Section 3, collaboration scenarios in PLM are analyzed and modeled; and QA-based collaboration mechanism as a promising solution is presented. Subsequently, mathematical models of secure collaboration mechanisms in PLM are proposed, and an instance of secure collaboration mechanism towards information inference is presented in Section 4. Finally, conclusions are given in Section 5.

2. PLM MATHEMATICAL MODEL

In this paper, axiomatic theory of design modeling is used to model the PLM.

2.1. Axiomatic Theory of Design Modeling

Axiomatic theory of design modeling is a logical tool for representing and reasoning about object structures [15]. It provides a formal approach that allows for the development of design theories following logical steps based on mathematical concepts and axioms. The primitive concepts of universe, object, and relation are used in this theory. A key concept in the axiomatic theory of design modeling is the structure operation, denoted by $\oplus$, which can be defined as the union $(\cup)$ of an object O and the interaction $(\otimes)$ of the object with itself.

$$\oplus O = O \cup (O \otimes O), \tag{1}$$

where the $\oplus O$ is the structure of object O.

Based on the structure operation, a product system can be defined as the structure of an object (Ω) that includes both a product (S) and it s environment (E). Here, the product is in its general sense.

$$\Omega = E \cup S, \forall E, S[E \cap S = \Phi], \tag{2}$$

where Φ is the object that is included in any object.

The product system ($\oplus \Omega$) can be expanded as follows:

$$\oplus \Omega = \oplus (E \cup S) = (\oplus E) \cup (\oplus S) \cup (E \otimes S) \cup (S \otimes E), \tag{3}$$

where $(\oplus E)$ and $(\oplus S)$ are structures of the environment and the product, respectively; $(E \otimes S)$ and $(S \otimes E)$ are the interactions between the environment and the product [15]. A product system can be illustrated in Figure 1.

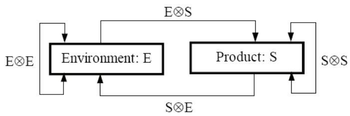

Figure 1. Product system [15]

Compared with other formalisms and models, such as Unified Modeling Language (UML), Structured Analysis and Design Technique (SADT), IDEF0/ IDEF3, axiomatic theory of design modeling is featured with knowledge-driven recursive design on a rather general, not specific, level, which aligns with the logic of design[16], by progressively exploring implied objects and their relations and describing dynamic system. Furthermore, it focused on the driving force of the functions by identified conflicts existing in the system, which encourage the creation of more available functions.

2.2. Formalization of PLM Systems

Axiomatic theory of design modeling forms the foundation for formalizing PLM systems. According to the axiomatic theory of design modeling, the structure of PLM, denoted by $\oplus S_{PLM}$, can be defined as the union of the product-centric objects like activities or processes or approaches, and the interaction of those objects between themselves. The structure of the environment of PLM is composed of all objects related to those product-centric objects and relations between objects and themselves and relations between objects, denoted by $\oplus E_{PLM}$. Therefore, PLM system consists of the structure of PLM and PLM environment, denoted by $\oplus \Omega_{PLM}$, that is,

$$\oplus \Omega_{PLM} = \oplus (E_{PLM} \cup S_{PLM}) = (\oplus E_{PLM}) \cup (\oplus S_{PLM}) \cup (E_{PLM} \otimes S_{PLM}) \cup (S_{PLM} \otimes E_{PLM}), \tag{4}$$

Environment can be generally classified into natural, built, and human environments, denoted by $\mathbf{E}^n$, E^b, and E^h, respectively [15].

$$\oplus E = \oplus \left(E^n \cup E^b \cup E^h\right). \tag{5}$$

In the environment of PLM, the natural environment includes objects such as *time, space, and natural resource*. The built environment includes objects such as *product, data, information, knowledge, methodology, technology tool, standards, organizations and business processes*. The human environment includes stakeholders such as *developers, suppliers*, *manufacturers*, *transporters, distributors, customers, maintainers, and recyclers*. Here, primitive components in the PLM environment can be selected.

- *Product (* $\mathrm{E_p}$): anything that can be offered to a market that might satisfy a need.
- *Product lifecycle (*$\mathrm{E_{pl}}$*):* a product property including phases such as development, production, distribution, operation and retirement.
- *Product data (*$\mathrm{E_{pd}}$*):* a product property comprising BOM, CAD/CAM models and so on [17].
- *Standards (*$\mathbf{E_{sd}}$*):* they can be classified into several typologies according to the stages of the product life cycle, the scope, the origin, the development process, and the intent [18].
- *Business processes (*$\mathrm{E_{bp}}$*):* product market strategy, product portfolio planning, product platform planning, customer requirements, product specification, conceptual design, detailed design, design analysis, prototyping and testing, process planning, inventory management, sourcing, production, inspection, packing, distribution, operation and service, disposal, and recycle [2, 19].
- *Technology tools (*$\mathbf{E_{tt}}$*):* CAD, CAPP, CAM, CAE, DMU, EDM, PDM, WFM, ERP, MRP, SCM, CRM, PM, etc [20].
- *Stakeholders* ($\mathrm{E_{sh}}$): developers, suppliers, manufacturers, transporters, distributors, customers, maintainers, and recyclers [21, 22].

Hence, the structure of PLM environment can be represented as the union of the structure of product, product lifecycle, product data, technology tools, standards, business processes, stakeholders and other primitive components ($\mathrm{E_o}$).

$$\oplus\, \mathrm{E_{PLM}} = \oplus \left(\mathrm{E^n_{PLM}} \cup \mathrm{E^b_{PLM}} \cup \mathrm{E^h_{PLM}}\right) = \oplus \left(\mathrm{E_p} \cup \mathrm{E_{pl}} \cup \mathrm{E_{pd}} \cup \mathrm{E_{tt}} \cup \mathrm{E_{sd}} \cup \mathrm{E_{bp}} \cup \mathrm{E_{sh}} \cup \mathrm{E_o}\right) \tag{6}$$

2.3. PLM Mathematical Model

In the environment of PLM, various relations exist between two components or from a component to itself, as shown in the Figure 2. Conflicts may emerge between two relations. For example, a relation that stakeholder A requires certain product data K triggers a conflict when the relation that stakeholder cannot access the data. Such conflict can be described by the following formulation,

$$c\left(e^A_{sh} \otimes_{\neg access} e^K_{pd}, e^A_{sh} \otimes_{require} e^K_{pd}\right). \tag{7}$$

To remove this conflict, available solutions have to be designed and performed until stakeholder A accesses the data K. Consequently, PLM can be regarded as a management process, providing a set of solutions consisted of a set of interrelated activities in order to address various unacceptable conflicts among the relations between the environment components of PLM system. A mathematical model of PLM is subsequently derived as follows,

$$\begin{cases} \oplus S_{PLM} = \oplus\, Solution_{\mathrm{PLM}} = \oplus\left(\bigcup_{i=1}^{n_s} s_i\right) = \bigcup_{i=1}^{n_s}(\oplus\, s_i) \cup \bigcup_{i_1=1}^{n_s}\bigcup_{\substack{i_2=1 \\ i_2\neq i_1}}^{n_s}\left(s_{i_1} \otimes s_{i_2}\right) \\ \oplus\, s_i = \bigcup_{j=1}^{n_a}(\oplus\, a_{ij}) \cup \bigcup_{j_1=1}^{n_a}\bigcup_{\substack{j_2=1 \\ j_2\neq j_1}}^{n_a}\left(a_{ij_1} \otimes a_{ij_2}\right), \forall s_i \subseteq Solution_{\mathrm{PLM}} \\ \exists s_i = \left\{\bigcup_{j=1}^{n_a} a_{ij} \middle| \begin{matrix} c_i \\ \mathrm{r}_i \end{matrix}\right\}, \forall a_{ij} \subseteq s_i \end{cases} \tag{8}$$

where c represents the conflict, r the resource of existing relations, s_i a sub-solution of the PLM solution. The sub-solution s_i is involved with activities that are in fact newly created relations to address the conflicts c_i among the original relations between the PLM environment components.
Thomas and Kilman identified five modes, or basic ways of addressing conflicts: accommodating, avoiding, competing, compromising, and collaboration [23]. Therein, collaboration is viewed as the only win-win solution to conflict, through mutual problem solving to satisfy both parties' needs. In the following two sections, we will focus on anatomizing the collaboration and secure collaboration based on this mathematical model of PLM systems.

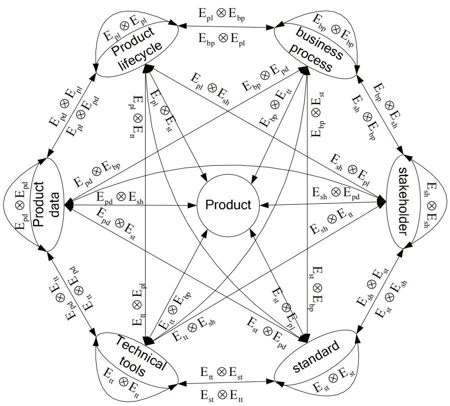

Figure 2. Relational graph in product lifecycle management environment

3. COLLABORATION MODELLING

3.1. Collaboration models

According to the mathematical model of PLM systems, the collaboration, as a kind of sub-solution of PLM, consists of a set of interrelated activities among objects in the environment of PLM. The structure of collaboration can be defined as the union of activities and the interactions of the activities between themselves. The environment of collaboration is composed of all objects related to those activities and relations of objects themselves and relations between objects. The structure and the environment of collaboration constitute the whole collaboration.
In PLM process, the collaboration between two stakeholders may happen in several settings for clarifying, sharing or changing product data. Here we list some possible scenarios as following:

1. *Stakeholder A e^A_{sh}, who can't access certain product data e^K_{pd}, requires the data privately owned by stakeholder B e^B_{pd}. For example, supplier needs to know a product parameter from designer.*

The conflict exists between the relation of *requirement* and *not access* between *stakeholder A* and *the product data K* as Equation (8). It can be removed through collaboration between *stakeholder A* and *stakeholder B, due to the existing relation of stakeholder B*'s own *the product data K.* Accordingly the solution *s* is formulized based on the above meta-model (see Equation (8)) as:

$$s = \left\{ Coll.\begin{pmatrix} e^A_{sh}\otimes e^B_{sh}, e^B_{sh}\otimes e^K_{pd}, \\ e^B_{sh}\otimes e^A_{sh}, e^A_{sh}\otimes e^K_{pd} \end{pmatrix} \middle| \begin{matrix} c\left(e^A_{sh}\otimes_{\neg access} e^K_{pd}, e^A_{sh}\otimes_{require} e^K_{pd}\right), \\ e^B_{sh}\otimes_{access} e^K_{pd} \end{matrix} \right\}, \qquad (9)$$
$$\forall e^A_{sh}, e^B_{sh} \subset E_{sh}, e^A_{sh} \neq e^B_{sh}, \forall e^K_{pd} \subset E_{pd}, e^K_{pd} \neq \Phi.$$

where $\text{Collaboration}\begin{pmatrix} e^A_{sh}\otimes e^B_{sh}, e^B_{sh}\otimes e^K_{pd}, \\ e^B_{sh}\otimes e^A_{sh}, e^A_{sh}\otimes e^K_{pd} \end{pmatrix}$ are one of the solutions of e^A_{sh} to access e^K_{pd} through e^B_{sh}.
Several activities may be involved in this collaboration solution, such as *stakeholder A* communicating with *stakeholder B, denoted by* $e^A_{sh} \otimes_{communicate} e^B_{sh}$, *stakeholder B accessing the product data K, denoted by* $e^B_{sh} \otimes_{access} e^K_{pd}$, *Stakeholder B* communicating with *Stakeholder*

A, , denoted by $e_{sh}^{B} \otimes_{communicate} e_{sh}^{A}$*, and stakeholder A* accessing *the product data K, denoted by* $e_{sh}^{A} \otimes_{access} e_{pd}^{K}$.

2. *Stakeholder B* e_{sh}^{B} *changes certain product data* e_{pd}^{B} *which should be consistent with certain product data* e_{pd}^{A} *owned by stakeholder A* e_{sh}^{A}*. For example, manufacturer changes product material due to lower cost of production while designer does not know it.*

The conflict $c(e_{sh}^{B} \otimes_{change} e_{pd}^{B}, e_{pd}^{A} \otimes_{consistent} e_{pd}^{B})$ arises between the relation of *stakeholder B* changing *product data* e_{pd}^{B} and relation of product *data* e_{pd}^{B} consistent *with product data* e_{pd}^{A}. It can be removed through collaboration between *stakeholder A* and *stakeholder B* until *Stakeholder A* change product data e_{pd}^{A}, Accordingly the solution is formulized as:

$$s = \left\{ Coll. \begin{pmatrix} e_{sh}^{A} \otimes e_{sh}^{B}, e_{sh}^{B} \otimes e_{pd}^{B}, \\ e_{sh}^{B} \otimes e_{sh}^{A}, e_{sh}^{A} \otimes e_{pd}^{A} \end{pmatrix} \middle| \begin{matrix} c(e_{sh}^{B} \otimes_{change} e_{pd}^{B}, e_{pd}^{A} \otimes_{consistent} e_{pd}^{B}), \\ e_{sh}^{B} \otimes_{own} e_{pd}^{B}, e_{sh}^{A} \otimes_{own} e_{pd}^{A} \end{matrix} \right\}, \quad (10)$$

$$\forall e_{sh}^{A}, e_{sh}^{B} \subset E_{sh}, e_{sh}^{A} \neq e_{sh}^{B}, \forall e_{pd}^{A}, e_{pd}^{B} \subset E_{pd}, e_{pd}^{A} \neq e_{pd}^{B}.$$

3. *Stakeholder B* e_{sh}^{B} *would like to change certain product data* e_{pd}^{K}*, but stakeholder A* e_{sh}^{A} *does not allow the change. For example, manufacturer changes product material due to lower cost of production while designer does not approve it.*

The conflict $c(e_{sh}^{B} \otimes_{change} e_{pd}^{K}, e_{sh}^{A} \otimes_{\neg change} e_{pd}^{K})$ exists between the relation of *stakeholder B* changing *product data* e_{pd}^{K} and the relation of *stakeholder A* e_{sh}^{A} not changing *product data* e_{pd}^{K}. Probable solution is that through negotiation between *stakeholder A* and *stakeholder B* until *product data* e_{pd}^{K} *mutually satisfy both parties, they both change the data*. Accordingly, the solution is formulized as:

$$s = \left\{ Coll. \begin{pmatrix} e_{sh}^{A} \otimes e_{sh}^{B}, e_{sh}^{B} \otimes e_{pd}^{K}, \\ e_{sh}^{A} \otimes e_{pd}^{K} \end{pmatrix} \middle| \begin{matrix} c(e_{sh}^{B} \otimes_{change} e_{pd}^{K}, e_{sh}^{A} \otimes_{\neg change} e_{pd}^{K}), \\ r(e_{sh}^{A} \otimes_{own} e_{pd}^{K}, e_{sh}^{B} \otimes_{own} e_{pd}^{K}) \end{matrix} \right\}, \quad (11)$$

$$\forall e_{sh}^{A}, e_{sh}^{B} \subset E_{sh}, e_{sh}^{A} \neq e_{sh}^{B}, \forall e_{pd}^{K} \subset E_{pd}, e_{pd}^{K} \neq \Phi.$$

4. *Stakeholder B* e_{sh}^{B} *would like to change certain product data* e_{pd}^{B} *of its own, which results in a change of certain product data* e_{pd}^{A} *owned by stakeholder A* e_{sh}^{A} *due to the logical dependence, but stakeholder A does not approve the change. For example, a supplier needs to know a parameter of the product from the designer.*

The conflict $c(e_{sh}^{B} \otimes_{change} e_{pd}^{B}, e_{sh}^{A} \otimes_{\neg change} e_{pd}^{A}, e_{pd}^{A} \otimes_{depend} e_{pd}^{B})$ exists among the relation of *Stakeholder B* changing its product data e_{pd}^{B}, the relation of *Stakeholder A not* changing its product data e_{pd}^{A}, and the relation of e_{pd}^{A} dependent on e_{pd}^{B}. Such conflict can be removed when *stakeholder A* negotiates with *stakeholder B,* with the result that either the changed product data e_{pd}^{A} and e_{pd}^{B} will be accepted respectively, or the dependency between product data e_{pd}^{A} and e_{pd}^{B} changes. Accordingly, the solution can be formulized as:

$$s = \left\{ Coll. \begin{pmatrix} e_{sh}^{A} \otimes e_{sh}^{B}, e_{sh}^{B} \otimes e_{pd}^{B}, \\ e_{sh}^{A} \otimes e_{pd}^{A}, e_{sh}^{A} \otimes e_{pd}^{B} \end{pmatrix} \middle| \begin{matrix} c\begin{pmatrix} e_{sh}^{B} \otimes_{change} e_{pd}^{B}, e_{sh}^{A} \otimes_{\neg change} e_{pd}^{A}, \\ e_{pd}^{A} \otimes_{depend} e_{pd}^{B} \end{pmatrix}, \\ r(e_{sh}^{A} \otimes_{own} e_{pd}^{A}, e_{sh}^{B} \otimes_{own} e_{pd}^{B}) \end{matrix} \right\}, \quad (12)$$

$$\forall e_{sh}^{A}, e_{sh}^{B} \subset E_{sh}, e_{sh}^{A} \neq e_{sh}^{B}, \forall e_{pd}^{A}, e_{pd}^{B} \subset E_{pd}, e_{pd}^{A} \neq e_{pd}^{B} \neq \Phi.$$

5. *Stakeholder B* e_{sh}^{B} *changes one of its own business process* e_{bp}^{B}*, which results in a necessary change of another business process* e_{bp}^{A} *possessed by stakeholder A* e_{sh}^{A}*, but stakeholder A does not approve the change. For example, delayed delivery of suppler results in the delayed assembly.*

The conflict $c(e_{sh}^{B} \otimes_{change} e_{bp}^{B}, e_{sh}^{A} \otimes_{\neg change} e_{bp}^{A}, e_{bp}^{A} \otimes_{depend} e_{bp}^{B})$ exists among the relation of *Stakeholder B* changing its *business process* e_{bp}^{B}, the relation of *Stakeholder A not* changing its *business processes* e_{bp}^{A}, and the relation of e_{bp}^{A} dependent on e_{bp}^{B}. The conflict can be removed when *stakeholder A* negotiates with *stakeholder B,* with the result that either the changed business process e_{bp}^{A} and e_{bp}^{B} will be accepted respectively, or the dependency between business process e_{bp}^{A} and e_{bp}^{B} changes. Accordingly, the solution can be formulized as Equation (13).

$$s = \left\{ Coll.\begin{pmatrix} e_{sh}^{A} \otimes e_{sh}^{B}, e_{sh}^{B} \otimes e_{bp}^{B}, \\ e_{sh}^{A} \otimes e_{bp}^{A}, e_{bp}^{A} \otimes e_{bp}^{B} \end{pmatrix} \middle| \, c\begin{pmatrix} e_{sh}^{B} \otimes_{change} e_{bp}^{B}, e_{sh}^{A} \otimes_{\neg change} e_{bp}^{A}, \\ e_{bp}^{A} \otimes_{depend} e_{bp}^{B} \end{pmatrix}, \; r\left(e_{sh}^{A} \otimes_{own} e_{bp}^{A}, e_{sh}^{B} \otimes_{own} e_{bp}^{B}\right) \right\}, \quad (13)$$

$$\forall e_{sh}^{A}, e_{sh}^{B} \subset E_{sh}, e_{sh}^{A} \neq e_{sh}^{B}, \forall e_{bp}^{A}, e_{bp}^{B} \subset E_{bp}, e_{bp}^{A} \neq e_{bp}^{B} \neq \Phi.$$

6. *Stakeholder A* e_{sh}^{A} *requires certain product data* e_{pd}^{K} *owned by stakeholder B* e_{sh}^{B} *through communication of respective technical tool.* Collaborations in PLM may happen without technical tools as the media; but in most cases, stakeholders collaborate with each other through technical tools as the media. *For example, manufacturer expects to obtain a product parameter from designer through communication of its product data management software with designer's computer-aided design software.*

The conflict, the same with that in the scenario 1, exists between the relation of *requirement* and *not access* between *stakeholder A* and *the product data K* as Equation (8). However, various available relations can generate different solutions to the same conflict. Here, we have known more relations. For example, *stakeholder* A can use *technical tool* e_{tt}^{A}; *stakeholder* B can use *technical tool* e_{tt}^{B}; and *technical tool* e_{tt}^{B} can access *product data* e_{pd}^{K}. Consequently, A series of processes can be designed: 1) stakeholder A inquire the product data from *stakeholder* B and stakeholder B agrees with him and 2) uses its technical tool 3) to access the data and 4) communicate with the technical tool of stakeholder A; 5) then, technical tool of stakeholder A can access the product data and 6) response to stakeholder A; 7) finally, stakeholder A can access the product data, which can remove the above conflict. Accordingly, this solution can be formalized as Equation (14).

$$s = \left\{ Coll.\begin{pmatrix} e_{sh}^{A} \otimes e_{sh}^{B}, e_{sh}^{B} \otimes e_{tt}^{B}, \\ e_{tt}^{B} \otimes e_{pd}^{K}, e_{tt}^{B} \otimes e_{tt}^{A}, \\ e_{tt}^{A} \otimes e_{pd}^{K}, e_{tt}^{A} \otimes e_{sh}^{A}, \\ e_{sh}^{A} \otimes e_{pd}^{K} \end{pmatrix} \middle| \, \begin{matrix} c\left(e_{sh}^{A} \otimes_{\neg access} e_{pd}^{K}, e_{sh}^{A} \otimes_{require} e_{pd}^{K}\right), \\ r\begin{pmatrix} e_{sh}^{B} \otimes_{use} e_{tt}^{B}, e_{tt}^{B} \otimes_{access} e_{pd}^{K}, \\ e_{sh}^{A} \otimes_{use} e_{tt}^{A} \end{pmatrix} \end{matrix} \right\}, \quad (14)$$

$$\forall e_{sh}^{A}, e_{sh}^{B} \subset E_{sh}, e_{sh}^{A} \neq e_{sh}^{B}, \forall e_{tt}^{A}, e_{tt}^{B} \subset E_{tt}, \forall e_{pd}^{K} \subset E_{pd}, e_{pd}^{K} \neq \Phi.$$

3.2. QA-based Collaboration mechanism

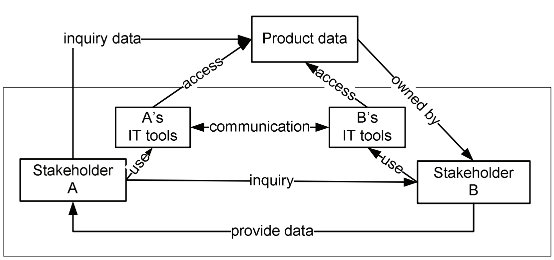

Figure 3. Collaboration between two stakeholders

For each scenario above, there are several kinds of unaccepted conflicts and consequently solutions should be developed. More prosaically, let's take the last scenario for example. According to our proposed method, the first step is to analyze the environment of collaboration. Following the manner of collaboration as shown in Fig. 3, human environment may be any two stakeholders, denoted by E_{sh}^{A} and E_{sh}^{B}, while the built environment should include the product data to be shared or clarified, denoted by E_{pd}^{K}, and A's IT tools E_{tt}^{A}, and B's IT tools E_{tt}^{B}. The major relations between those environment components are listed in Table 1.

Table 1. Major relations in collaboration

$E_{sh}^{A} \otimes E_{sh}^{B}$	Inquiry	$E_{sh}^{B} \otimes E_{sh}^{A}$	response, filter
$E_{tt}^{A} \otimes E_{tt}^{B}$	Communication	$E_{tt}^{B} \otimes E_{tt}^{A}$	communication
$E_{sh}^{A} \otimes E_{pd}^{B}$	not access, require, inquiry	$E_{sh}^{B} \otimes E_{pd}^{K}$	own, prepare, process
$E_{sh}^{A} \otimes E_{tt}^{A}$	Use	$E_{sh}^{B} \otimes E_{tt}^{B}$	use
$E_{tt}^{A} \otimes E_{pd}^{K}$	access	$E_{tt}^{B} \otimes E_{pd}^{K}$	access

The second step is to recognize the unaccepted conflicts among those relations. To resolve one of the conflicts, such as $c\left(e_{sh}^{A} \otimes_{\neg access} e_{pd}^{K}, e_{sh}^{A} \otimes_{require} e_{pd}^{K} \right)$, several collaboration mechanisms for this scenario will be proposed, such as establishing software interface and asking-right questions. Question asking has been proved not only as a process and as creative negotiation, but also as a mechanism for managing convergent and divergent thinking modes [24]. It has been mature contrastively with research, methods and even tools. Wang and Zeng have proposed a systematic iterative question-asking approach to clarify and elicit text information [25]. This approach aims at identifying the actor's real intent and at capturing the complete information by asking questions based on a semantic analysis of the given text. This strategy, as a recursive collaboration mechanism, can be selected for formulization in the third step:

$$s = \left\{ Coll. \left(\begin{array}{c} e_{sh}^{A} \otimes_{prepare} e_{pd}^{Q_1} \to e_{sh}^{A} \otimes_{ask} e_{sh}^{B} \\ \to e_{sh}^{B} \otimes_{prepare} e_{pd}^{A_1} \to e_{sh}^{B} \otimes_{response} e_{sh}^{A} \\ \to e_{sh}^{A} \otimes_{use} e_{tt}^{QGT} \to e_{tt}^{QGT} \otimes_{response} e_{pd}^{Q_2} \\ \to e_{sh}^{A} \otimes_{ask} e_{sh}^{B} \to e_{sh}^{B} \otimes_{prepare} e_{pd}^{A_2} \\ \to \cdots \to e_{sh}^{B} \otimes_{prepare} e_{pd}^{A_n} \to e_{sh}^{B} \otimes_{response} e_{sh}^{A} \end{array} \right) \middle| \begin{array}{c} c\left(\begin{array}{c} e_{sh}^{A} \otimes_{\neg access} e_{pd}^{K}, \\ e_{sh}^{A} \otimes_{require} e_{pd}^{K} \end{array} \right), \\ r\left(\begin{array}{c} e_{tt}^{B} \otimes_{access} e_{pd}^{K}, \\ e_{sh}^{A} \otimes_{use} e_{tt}^{QGT}, \ldots \end{array} \right) \end{array} \right\}, \quad (15)$$

$$\forall e_{sh}^{A}, e_{sh}^{B} \subset E_{sh}, e_{sh}^{A} \neq e_{sh}^{B}, \forall e_{tt}^{QGT} \subset E_{tt}, \forall e_{pd}^{A_1}, e_{pd}^{A_2}, \ldots, e_{pd}^{A_n}, e_{pd}^{K} \subset E_{pd}, e_{pd}^{K} \neq \Phi, e_{pd}^{K} \subset e_{pd}^{A_n}.$$

where e_{tt}^{QGT} is question generation tool. In this model, stakeholder A and its IT tools are abstracted to "question answer"; stakeholder B and its IT tools are abstracted to "question asker"; product data are abstracted to product parameters and relations among these product parameters. According to the analysis and the formulization, this question asking approach is validated as an effective solution to remove the conflict. Therefore, it is suitable for the inquiry based collaboration in the product lifecycle management, through which the collaborative partners may clarify and share information, and even get coordinated during the whole PLM process.

4. SECURE COLLABORATION MODELLING

4.1. Secure Collaboration Models

The conflict between protecting and accessing product data is the major reason of most security issues in a PLM environment. The secure collaboration issue can be portrayed as a scenario in which one stakeholder may try to protect a particular set of product data while other stakeholders expect to access it. In the PLM environment, three components, stakeholders (E_{sh}), technical tools (E_{tt}) and product data (E_{pd}), are directly relevant to secure collaborations. According to the manner of secure collaboration shown in Figure 4, human environment may involve any two stakeholders of the developers, suppliers, manufacturers, transporters, distributors, customers, maintainers, and recyclers or information systems. Here we denote them by E_{sh}^{A} and E_{sh}^{B}. And the built environment here involves the product data to be shared or clarified, and the product data to be protected, respectively denoted by E_{pd}^{P} and E_{pd}^{S}, as well as A's IT tools E_{tt}^{A}, and B's IT tools E_{tt}^{B}. Table 2 draws some major relations between these environment components relevant to secure collaborations.

Table 2. Major relations relevant to secure collaboration

$E_{sh} \otimes E_{pd}$	Protection, Access	$E_{tt} \otimes E_{tt}$	Communication
$E_{tt} \otimes E_{pd}$	Access	$E_{sh} \otimes E_{sh}$	Inquiry, Response, Communication
$E_{sh} \otimes E_{tt}$	Access	$E_{pd} \otimes E_{pd}$	Inference, Dependency

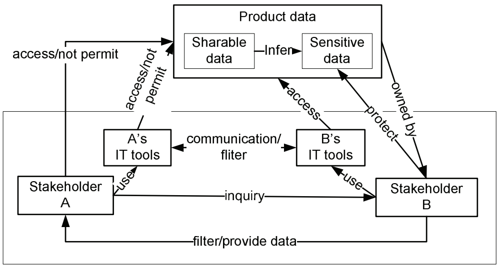

Figure 4. Secure collaboration between two stakeholders

For the purpose of protecting the intellectual properties contained in product data, the stakeholder who owns the product data has to restrict other stakeholder's accesses to its product data during collaborations in PLM. Therefore, first, we will analyze how a stakeholder can access another stakeholder's product data; and then try to find corresponding protections to possible access routes, as shown in Fig. 5.

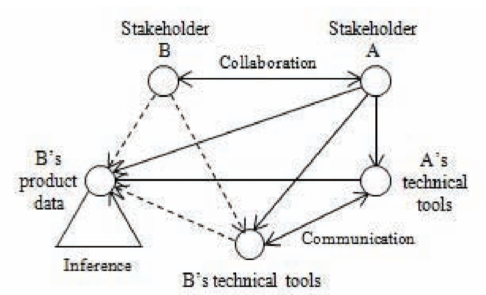

Figure 5. Possible access routes

1. *Stakeholder A may access stakeholder B's sensitive and sharable product data directly. For example, stakeholder A may read stakeholder B's product data from drawings of the product on paper.*

Security collaboration mechanisms for this access route can be described in Equation (16).

$$S = \left\{ S.C.\begin{pmatrix} e_{sh}^{B} \otimes e_{pd}^{S}, e_{sh}^{B} \otimes e_{pd}^{P}, \\ e_{sh}^{A} \otimes e_{pd}^{P} \end{pmatrix} \middle| \begin{matrix} c\left(e_{sh}^{B} \otimes_{protect} e_{pd}^{S}, e_{sh}^{A} \otimes_{access} e_{pd}^{S}\right), \\ r\left(e_{sh}^{B} \otimes_{own} e_{pd}^{S}, e_{sh}^{B} \otimes_{own} e_{pd}^{P}\right) \end{matrix} \right\}, \tag{16}$$

$$\forall e_{sh}^{A}, e_{sh}^{B} \subset E_{sh}, e_{sh}^{A} \neq e_{sh}^{B}, \forall e_{pd}^{P}, e_{pd}^{S} \subset E_{pd}, e_{pd}^{P} \neq e_{pd}^{S} \neq \Phi.$$

where c represents the conflict, $SC\left(e_{sh}^{B} \otimes e_{pd}^{S}, e_{sh}^{B} \otimes e_{pd}^{P}, e_{sh}^{A} \otimes e_{pd}^{P}\right)$ are the security collaboration solution of e_{sh}^{B} sharing the product data e_{pd}^{P} while protecting the sensitive data e_{pd}^{S} from e_{sh}^{A}. Secure collaboration mechanisms for restricting this access route may contain bureaucratic methods and BLP security model, focusing on the relation of $e_{sh}^{B} \otimes e_{pd}^{S}$.

2. *Stakeholder A may access stakeholder B's product data through stakeholder B's technical tools. In this case, the product data are usually in electronic formats and managed by stakeholder B's technical tools.*

Secure collaboration mechanisms for restricting this access route may contain authentication, authorization and role based access control, focusing on the relation of $e_{sh}^{A} \otimes e_{tt}^{B}$ and $e_{tt}^{B} \otimes e_{pd}^{S}$. Secure collaboration mechanisms for this access route can be described in Equation (17).

$$s=\left\{S.C.\begin{pmatrix} e_{sh}^{A}\otimes e_{tt}^{B}, e_{tt}^{B}\otimes e_{pd}^{P},\\ e_{tt}^{B}\otimes e_{pd}^{S}, e_{sh}^{A}\otimes e_{pd}^{P}\end{pmatrix}\middle|\begin{matrix} c\left(e_{sh}^{B}\otimes_{protect} e_{pd}^{S}, e_{sh}^{A}\otimes_{access} e_{tt}^{B}, e_{tt}^{B}\otimes_{access} e_{pd}^{S}\right),\\ r\left(e_{sh}^{B}\otimes_{own} e_{pd}^{S}, e_{sh}^{B}\otimes_{own} e_{pd}^{P}, e_{sh}^{A}\otimes_{communicate} e_{sh}^{B}\right)\end{matrix}\right\} \quad (17)$$

$$\forall e_{sh}^{A}, e_{sh}^{B}\subset E_{sh}, e_{sh}^{A}\neq e_{sh}^{B}, \forall e_{pd}^{P}, e_{pd}^{S}\subset E_{pd}, e_{pd}^{P}\neq e_{pd}^{S}\neq \Phi, \forall e_{tt}^{B}\subset E_{tt}.$$

3. *Stakeholder A may access its own technical tools first, and then stakeholder A's technical tools access stakeholder A's product data directly.*

Similar to last access route, secure collaboration mechanisms for restricting this access route may contain authentication, authorization and role based access control too, focusing on the relation of $e_{sh}^{A}\otimes e_{tt}^{A}$ and $e_{tt}^{A}\otimes e_{pd}^{S}$. Secure collaboration mechanisms for this access route can be described as:

$$s=\left\{S.C.\begin{pmatrix} e_{sh}^{A}\otimes e_{tt}^{A}, e_{tt}^{A}\otimes e_{pd}^{P},\\ e_{tt}^{A}\otimes e_{pd}^{S}, e_{sh}^{A}\otimes e_{pd}^{P}\end{pmatrix}\middle|\begin{matrix} c\left(e_{sh}^{B}\otimes_{protect} e_{pd}^{S}, e_{sh}^{A}\otimes_{access} e_{tt}^{A}, e_{tt}^{A}\otimes_{access} e_{pd}^{S}\right),\\ r\left(e_{sh}^{B}\otimes_{own} e_{pd}^{S}, e_{sh}^{B}\otimes_{own} e_{pd}^{P}, e_{sh}^{A}\otimes_{communicate} e_{sh}^{B}\right)\end{matrix}\right\}, \quad (18)$$

$$\forall e_{sh}^{A}, e_{sh}^{B}\subset E_{sh}, e_{sh}^{A}\neq e_{sh}^{B}, \forall e_{pd}^{P}, e_{pd}^{S}\subset E_{pd}, e_{pd}^{P}\neq e_{pd}^{S}\neq \Phi, \forall e_{tt}^{A}\subset E_{tt}.$$

4. *Stakeholder A may access its own technical tools first, and then access stakeholder B's product data through communication with stakeholder B's technical tools.*

Secure collaboration mechanisms for restricting this access route may contain authentication, authorization and role based access control, dealing with the rations of $e_{sh}^{A}\otimes e_{tt}^{A}$, $e_{tt}^{A}\otimes e_{tt}^{B}$, $e_{tt}^{B}\otimes e_{pd}^{S}$. Secure collaboration mechanisms for this access route can be described in Equation (19).

$$s=\left\{S.C.\begin{pmatrix} e_{sh}^{A}\otimes e_{tt}^{A}, e_{tt}^{A}\otimes e_{tt}^{B},\\ e_{tt}^{B}\otimes e_{pd}^{P}, e_{tt}^{B}\otimes e_{pd}^{S},\\ e_{tt}^{B}\otimes e_{tt}^{A}, e_{tt}^{A}\otimes e_{pd}^{P},\\ e_{tt}^{A}\otimes e_{sh}^{A}, e_{sh}^{A}\otimes e_{pd}^{P}\end{pmatrix}\middle|\begin{matrix} c\begin{pmatrix} e_{sh}^{B}\otimes_{protect} e_{pd}^{S}, e_{sh}^{A}\otimes_{access} e_{tt}^{A},\\ e_{tt}^{A}\otimes_{communicate} e_{tt}^{B}, e_{tt}^{B}\otimes_{access} e_{pd}^{S}\end{pmatrix},\\ r\begin{pmatrix} e_{sh}^{B}\otimes_{own} e_{pd}^{S}, e_{sh}^{B}\otimes_{own} e_{pd}^{P},\\ e_{sh}^{B}\otimes_{access} e_{tt}^{B}, e_{tt}^{B}\otimes_{access} e_{pd}^{P}\\ e_{sh}^{A}\otimes_{communicate} e_{sh}^{B}\end{pmatrix}\end{matrix}\right\}, \quad (19)$$

$$\forall e_{sh}^{A}, e_{sh}^{B}\subset E_{sh}, e_{sh}^{A}\neq e_{sh}^{B}, \forall e_{pd}^{P}, e_{pd}^{S}\subset E_{pd}, e_{pd}^{P}\neq e_{pd}^{S}\neq \Phi, \forall e_{tt}^{A}, e_{tt}^{B}\subset E_{tt}.$$

5. *Since stakeholder B can access its own product data, stakeholder A may access stakeholder B's product data through collaboration with stakeholder B.*

The collaboration between two stakeholders is a asking and answering process in Figure 4. Therefore, secure collaboration mechanisms for restricting this access route can be regarded as a decision-making problem focusing on the relation $e_{sh}^{B}\otimes e_{sh}^{A}$ and $e_{tt}^{B}\otimes e_{pd}^{S}$. When a question asker asks a product parameter, the question answer has to make a decision on how to answer the question. Secure collaboration mechanisms for this access route can be described in Equation (20).

$$s=\left\{S.C.\begin{pmatrix} e_{sh}^{A}\otimes e_{sh}^{B}, e_{sh}^{B}\otimes e_{tt}^{B}, e_{tt}^{B}\otimes e_{pd}^{P}\\ e_{tt}^{B}\otimes e_{pd}^{S}, e_{tt}^{B}\otimes e_{sh}^{B}, e_{sh}^{B}\otimes e_{pd}^{P},\\ e_{sh}^{B}\otimes e_{pd}^{S}, e_{sh}^{B}\otimes e_{sh}^{A}, e_{sh}^{A}\otimes e_{pd}^{P}\end{pmatrix}\middle|\begin{matrix} c\left(e_{sh}^{B}\otimes_{protect} e_{pd}^{S}, e_{sh}^{A}\otimes_{access} e_{pd}^{S}\right),\\ r\begin{pmatrix} e_{sh}^{B}\otimes_{own} e_{pd}^{S}, e_{sh}^{B}\otimes_{own} e_{pd}^{P},\\ e_{sh}^{B}\otimes_{access} e_{tt}^{B}, e_{tt}^{B}\otimes_{access} e_{pd}^{P},\\ e_{tt}^{B}\otimes_{access} e_{pd}^{S}, e_{sh}^{A}\otimes_{communicate} e_{sh}^{B}\end{pmatrix}\end{matrix}\right\} \quad (20)$$

$$\forall e_{sh}^{A}, e_{sh}^{B}\subset E_{sh}, e_{sh}^{A}\neq e_{sh}^{B}, \forall e_{pd}^{P}, e_{pd}^{S}\subset E_{pd}, e_{pd}^{P}\neq e_{pd}^{S}\neq \Phi, \forall e_{tt}^{B}\subset E_{tt}.$$

6. *After stakeholder A gets a set of shared product data, it may infer from this set of product data to other sensitive product data by physical and logical dependency relations among these product data.*

To restrict this access route, risk evaluation of information leakage is required. Secure collaboration mechanisms for this access route either focusing on relation of $e_{sh}^{B}\otimes e_{pd}^{P}$ and $e_{pd}^{P}\otimes e_{pd}^{S}$, which can be described in Equation (21).

$$s=\left\{S.C.\begin{pmatrix} e_{pd}^{P}\otimes e_{pd}^{S}, e_{sh}^{A}\otimes e_{pd}^{P}, \\ e_{sh}^{B}\otimes e_{pd}^{S} \end{pmatrix}\middle| \begin{matrix} c\left(e_{sh}^{B}\otimes_{protect} e_{pd}^{S}, e_{sh}^{A}\otimes_{access} e_{pd}^{P}, e_{pd}^{P}\otimes_{infer} e_{pd}^{S}\right), \\ r\left(e_{sh}^{B}\otimes_{own} e_{pd}^{S}, e_{sh}^{B}\otimes_{own} e_{pd}^{P}, e_{sh}^{A}\otimes_{communicate} e_{sh}^{B}\right) \end{matrix}\right\} \quad (21)$$

$$\forall e_{sh}^{A}, e_{sh}^{B}\subset E_{sh}, e_{sh}^{A}\neq e_{sh}^{B}, \forall e_{pd}^{P}, e_{pd}^{S}\subset E_{pd}, e_{pd}^{P}\neq e_{pd}^{S}\neq \Phi.$$

4.2. Evaluation-based Secure Collaboration Mechanism for Information Inference

For the last secure collaboration mechanism as mentioned above, to facilitate collaboration, manufacturers usually share non-private information with their partners, suppliers and customers while trying to keep private information confidential. However, they cannot adequately prevent the leakage of confidential information caused by reverse engineering. Therefore, there is such a possibility that partners, suppliers or customers may be able to infer confidential information from shared non-private information and inherent engineering relationships existing between them. With the increase of the amount of information that a partner, supplier or customer may obtain on a particular product, the possibility will increase that the confidential information is inferred. To protect its product data, a stakeholder (manufacture) has to find an optimal solution that allocates components to other stakeholders (possible partners and/or suppliers), in which the risks of information leakage are underneath a specific degree. Our research group proposed a graph tool, Logical Dependency Graph [26], to describe the logical dependencies among product data, and a method to evaluate the risks of information leakage based on Logical Dependency Graph. The first step in the generic protection process protecting is to find all possible allocations from components to their suppliers. For a particular allocation, represented by Equation (22) based on the secure collaboration model in Equation (21), the manufacture e_{sh}^{B} will share corresponding parameters with its partners and suppliers. It forms a share schema, which defines what parameters are shared with each partner or supplier e_{sh}^{A}. If e_{sh}^{A} is shared with too many product parameters, it may infer some private parameters e_{pd}^{P} from these shared parameters e_{pd}^{K}. Therefore, we want to know the probability of information leakage for each allocation and corresponding share schema. When the risks are lower than a particular value e_{sd}^{Risk}, the allocation and corresponding information share schema are considered safe; otherwise, some approaches may be taken to mitigate the risks. After the above steps, the manufacturer will get some allocations and corresponding information share schemas whose risks of information leakage are underneath a specific degree.

$$s=\left\{S.C.\begin{pmatrix} e_{sh}^{A}\otimes_{inquire} e_{pd}^{K}\rightarrow e_{sh}^{B}\otimes_{prepare} e_{pd}^{K} \\ \rightarrow e_{sh}^{B}\otimes_{set} e_{sd}^{Risk} \\ \rightarrow\left(e_{sh}^{B}\otimes_{evaluate}\left(e_{pd}^{K}\otimes_{infer} e_{pd}^{P}\right)\right)\otimes_{compare} e_{sd}^{Risk} \\ \rightarrow e_{sh}^{B}\otimes_{response} e_{pd}^{S} \end{pmatrix}\middle| \begin{matrix} c\begin{pmatrix} e_{sh}^{B}\otimes_{protect} e_{pd}^{S}, \\ e_{sh}^{A}\otimes_{access} e_{pd}^{P}, \\ e_{pd}^{P}\otimes_{infer} e_{pd}^{S} \end{pmatrix}, \\ r\begin{pmatrix} e_{sh}^{B}\otimes_{own} e_{pd}^{S}, \\ e_{sh}^{B}\otimes_{own} e_{pd}^{P}, \\ e_{sh}^{A}\otimes_{comm.} e_{sh}^{B}, \\ \dots \end{pmatrix} \end{matrix}\right\}, \quad (22)$$

$$\forall e_{sh}^{A}, e_{sh}^{B}\subset \mathrm{E}_{sh}, e_{sh}^{A}\neq e_{sh}^{B}, \forall e_{pd}^{P}, e_{pd}^{S}\subset \mathrm{E}_{pd}, e_{pd}^{P}\neq e_{pd}^{S}\neq \Phi, e_{sd}^{Risk}\subset \mathrm{E}_{sd}$$

This model described the available resources (objects and relations) in the PLM, and identified the potential conflicts existing in the scenario of information leakage by inference, which can be mitigated through the presented process. It is also implied that more possible secure collaboration mechanisms could be generated with more conflicts observation when resources are changing.

5. CONCLUSION

In this paper, a mathematical model of PLM is developed to represent the formalization of product lifecycle management systems. The foundation of this mathematical model is the axiomatic theory of design modeling. It provides a process to formulize product lifecycle management by environment components identification, relations and conflicts analysis, and solutions generation. Accordingly, the concept of product lifecycle management is redefined as a union of solutions consisted of a set of interrelated activities or mechanisms addressing various unacceptable conflicts among the relations between the product centric environment components in its system from the design point of view. The proposed mathematical model of PLM systems is derived from the structure of PLM solutions, activities, conflicts, environment components and their relations.

To verify and apply PLM mathematical meta-model, we focus on the collaboration and secure collaboration issues. Six collaboration scenarios in PLM are proposed, and conflicts among the relations in each scenario are identified to derive possible solutions, which are modeled to develop the mathematical model of PLM systems. After that, a secure collaboration scenario in PLM is proposed, where secure collaboration mechanisms for the six possible collaboration routes are modeled. Finally, a method of evaluating the risks of information leakage is used as a secure collaboration mechanism toward the information inference for the validation of the proposed secure collaboration model.

The mathematical model of PLM systems will be developed in the future work through mathematical modeling integration, product information and business processes, etc., with more primitive environment components, relations and conflicts being investigated. Furthermore, another ongoing research of our lab is devoted to the real application of the secure collaboration mechanisms to five collaborating aerospace manufacturing companies.

ACKNOWLEDGEMENTS

The research presented in this paper is supported by NSERC-CRD (PJ 350114-06). We are grateful to the financial support from NSERC, CRIAQ, Pratt & Whitney Canada Corp, Bombardier Inc., CAE Inc., CMC Electronics Inc., and Rolls-Royce Canada Limited. The first author is partially supported by CSC (The China Scholarship Council).

REFERENCES

[1] Sääksvuori, A. and A. Immonen, *Product lifecycle management*, 2 ed, *Vol*. 2005 (Springer, Berlin, London).

[2] Ming, X.G., J.Q. Yan, et al., Technology solutions for collaborative product lifecycle management - Status review and future trend. *Concurrent Engineering-Research and Applications*, 2005, 13(4), 311-319.

[3] Ameri, F. and D. Dutta, Product Lifecycle Management Needs, Concepts and Components. 2004, University of Michigan, Ann Arbor, MI, pp. 2.

[4] Hartmann, G., *Product lifecycle management with SAP: The complete guide to my SAP PLM strategy, Technology and best practices*, *Vol*. 2005 (SAP Press).

[5] Sudarsan, R., S.J. Fenves, et al., A product information modeling framework for product lifecycle management. *Computer-Aided Design*, 2005, 37(13), 1399-1411.

[6] Lee, Y.-C., L.-C. Sheu, and Y.-G. Tsou, Quality function deployment implementation based on Fuzzy Kano model: An application in PLM system. *Computers & Industrial Engineering*, 2008, 55(1), 48-63.

[7] Abramovici, M., Digital Engineering und PLM - Zwei unterschiedliche Ansätze? in *Digital Engineering Magazin*, 2005.

[8] Sun, D.W., X.H. Xiong, et al. Workflow-driven collaborative session management in product lifecycle management via Internet. in *Engineering Management Conference, 2004. Proceedings. 2004 IEEE International*, 2004,pp. 1146-1150 Vol.3.

[9] Gruat La Forme, F.-A., V.B. Genoulaz, and J.-P. Campagne, A framework to analyse collaborative performance. *Computers in Industry*, 2007, 58(7), 687-697.

[10] Leong, K.K., K.M. Yu, and W.B. Lee, A security model for distributed product data management system. *Computers in Industry*, 2003, 50(2), 179-193.

[11] Cera, C.D., T. Kim, et al., Role-based viewing envelopes for information protection in collaborative modeling. *Computer-Aided Design*, 2004, 36(9), 873-886.

[12] Cera, C.D., I. Braude, et al., Hierarchical Role-Based Viewing for Multilevel Information Security in Collaborative CAD. *Journal of Computing and Information Science in Engineering*, 2006, 6(1), 2-10.

[13] Kim, T., C.D. Cera, et al., Multi-Level modeling and access control for data sharing in collaborative design. *Advanced Engineering Informatics*, 2006, 20(1), 47-57.

[14] Wang, Y., P.N. Ajoku, et al., Intellectual Property Protection in Collaborative Design through Lean Information Modeling and Sharing. *Journal of Computing and Information Science in Engineering*, 2006, 6(2), 149-159.

[15] Zeng, Y., Axiomatic theory of design modeling. *Transaction of SDPS: Journal of Integrated Design and Process Science*, 2002, 6(3), 1-28.
[16] Zeng, Y. and G.D. Cheng, On the logic of design. *Design Studies*, 1991, 12(3), 137-141.
[17] Thimm, G., Y.-S. Ma, et al. An investigation into the early and retirement life-cycle stages: tools, requirements. in *International Conference on Product Lifecycle Management (PLM07)*, Politecnico di Milano, 2007.
[18] Rachuri, S., E. Subrahmanian, et al., Information sharing and exchange in the context of product lifecycle management: Role of standards. *Computer-Aided Design*, 2008, 40(7), 789-800.
[19] Ullman, D.G., *The Mechanical Design Process*, *Vol*. 1997 (McGraw-Hill, New York).
[20] Terzi, S., Elements of Product Lifecycle Management: Definitions, Open Issues and Reference Models. 2005, l'Université Henri Poincaré Nancy I en cotutelle avec le Politecnico di Milano.
[21] Ming, X.G., J.Q. Yan, et al., Mass production of tooling product families via modular feature-based design to manufacturing collaboration in PLM. *Journal of Intelligent Manufacturing*, 2007, 18(1), 185-195.
[22] Smirnov, A., M. Pashkin, et al., Ontology-based support for semantic interoperability between SCM and PLM. *International Journal of Product Lifecycle Management*, 2006, 1(3), pp.289-302.
[23] Thomas, K.W. and R.H. Kilmann, *Thomas-Kilmann Conflict Mode instrument*, *Vol*. 1974 (Xicom, Tuxedo, NY).
[24] Eris, Ö., *Effective inquiry for innovative engineering design*, *Vol*. 2004 (Stanford University: Kluwer Academic Publishers).
[25] Ming, X.G., J.Q. Yan, et al., Collaborative process planning and manufacturing in product lifecycle management. *Computers in Industry*, 2008, 59(2-3), 154-166.
[26] Zhang, D.Y., Y. Zeng, et al., Risk Evaluation of Confidential Information Leakage in Collaborative New Product Development. 2009, Concordia Institute for Information Systems Engineering, Concordia University: Montreal, Quebec, Canada.

Contact: Yong Zeng
Concordia University
Concordia Institute for Information Systems Engineering
1455 de Maisonneuve West, EV.07.633
H3G 1M8, Montreal
Canada
Phone: +1-514-848-2424 #5801
Fax: +1-514-848-3171
E-mail: zeng@ciise.concordia.ca
URL: http://users.encs.concordia.ca/~zeng/index.html

Dr. Yong Zeng is an Associate Professor in the Concordia Institute for Information Systems Engineering at Concordia University, Montreal, Canada. He received his B.Eng. degree in structural engineering from the Institute of Logistical Engineering and M.Sc. and Ph.D degrees in computational mechanics from Dalian University of Technology in 1986, 1989, and 1992, respectively. He received his second Ph.D. degree in design engineering from the University of Calgary in 2001. His research interests include the science of design, requirements engineering, human factors engineering, computer-aided product development, product lifecycle management, computational geometry, and finite element modeling.