International Journal of Mechanical, Industrial and Aerospace Sciences
ISSN: 2517-9950
Vol:6, No:8, 2012

Enhanced Data Access Control of Cooperative Environment used for DMU Based Design

Wei Lifan, Zhang Huaiyu, Yang Yunbin, Li Jia

***Abstract*—**Through the analysis of the process digital design based on digital mockup, the fact indicates that a distributed cooperative supporting environment is the foundation conditions to adopt design approach based on DMU. Data access authorization is concerned firstly because the value and sensitivity of the data for the enterprise. The access control for administrators is often rather weak other than business user. So authors established an enhanced system to avoid the administrators accessing the engineering data by potential approach and without authorization. Thus the data security is improved.

***Keywords*—**access control, DMU, PLM, virtual prototype.

I. Introduction

DEVELOPING complex system satisfied the requirements in a reasonable period and cost limiting is a serious challenge. A lot of techniques and methods have been developed towards this target. The core feature of these approaches is cooperation and simulation.

Digital mockup technique represents an important role in the process of product development. With the help of digital mockup, it becomes realization to make a lot of virtual prototypes used for simulating and evaluating during the various phases of the product lifecycle. The virtual prototype is used for explaining the product design, simulating the function of product, evaluating the performance of the product in the product design stage. And it also could be helpful to explain the structure and function of the product, the approach of maintenance in product commission stage [1].

The origin concept of virtual prototype is to establish a model in computer to delegate some features of the physical prototype. Virtual prototype is always established separately with the physical prototype in a digital virtual environment in computer. This technique helps to avoid the expensive cost and time for construction physical prototype [2] [3].

One of the most benefits of virtual prototype for product development is the ability to establish the prototype in the early design stage.

Wei Lifan is with the Institute of Structural Mechanics, China Academy of Engineering Physics, MianYang, Sichuan, 621900,China ((phone: 86-0816-2281485; fax: 86-0816-2281485 ; e-mail: weilifan@ caep.ac.cn).

Zhang Huaiyu is with the Institute of Structural Mechanics, China Academy of Engineering Physics, P.Box.411, MianYang, Sichuan, 621900,China (phone: 86-0816-2281485; fax: 86-0816-2281485).

Yang Yunbin is with the Institute of Structural Mechanics, China Academy of Engineering Physics, P.Box.411, MianYang, Sichuan, 621900,China (phone: 86-0816-2281485; fax: 86-0816-2281485; e-mail: yyb717@163.com).

Li Jia is with the Institute of Structural Mechanics, China Academy of Engineering Physics, P.Box.411, MianYang, Sichuan, 621900,China (phone: 86-0816-2281485; fax: 86-0816-2281485).

So the evaluation of the prototype could advise on the design in time [4] [5]. Another obvious benefit of virtual prototype is one could constructs the prototype in the computer time and again with very little cost.

The overall virtual prototype aims to replace the physical prototype. This goal is achieved currently only in some special domains. For many kinds product, only portion feature or features is simulated to support design. A cooperative environment is necessary for such a process of design on DMU. Some feature of such an environment was discussed [1], the effect of the environment is similar for cooperative design platform.

In general, such an environment helps the companies manage the product data and development process. The digital mockup evolves continuously during the product development process. Everyone works on it through the cooperative system. Experts in different domains work on the source data represents by the digital mockup, and submit their achievements into the cooperating platform. So the information accompanies with the digital mockup becomes abundant more and more.

A cooperative working environment becomes the basis condition for developing product based on digital mockup. The product development process accompanies with the process to define the digital model of the product. This definition process involves the design stages such as requirement analysis, scheme design, geometry design, technologic design and performance simulating and so on. Everyone gets his input from another person's working through the primitive digital model of product, and makes the model more detail in a cooperative working status. In such a cooperative development process, the sharing of product information in an effective way is concerned primarily. This means not only the conveniences for persons with authorization to access the product data, but also the grimly limitation for persons without authorization.

A cooperative working environment often establishes on some commercial PLM software which will provides the approach to control data access. In such working environment, the data access control aimed at the business user is often consummate. But for administration user, there is always some underlying approach to break through the data access control. Because the administration users often have some absolute privileges, they always have more approach to access the data without formal authority.

For a practical cooperative working environment, the potential approach to access data that evade the authority is always unacceptable. Because the data and knowledge preserved in such a platform are often the kernel intelligent asset of a company.

The exposure of such information is always will damage the competition efficiency of the company severely. Sometimes, it is the most concerned issue to keep the engineering data away from access without authority. Therefore, the technical measures to avoid potential avenues for access to engineering data by system administrators are really needed. This can enhance the effect of the data access control system to improve data security.

Designing methods based on digital mockup is adopted in many companies, included the institute authors serviced. A cooperative working environment is established to support the studying and applying of DMU. And an enhanced system to control the data access is established to keep the data safety. Even if one of the administrators the supporting system, would have no chance to access engineering data without authority. The security of the product data is improved evidently.

II. Design approach based on DMU

The essential of product development is to determine the design model and make it real. The design model is established iteratively with estimation round and round. The design model should be transformed into the real product with prospective way, and the product will works in the expected way.

Digital mockup technique is a suitable method to describe the design model of a product. It is the appropriate carrier to transfer information among the various simulation activities. And it evolves itself because the evaluations give more and more design advises. Digital mockup is used in all stages of the product lifecycle, although it has some different characterization because the special concerns. The overall digital mockup is expected to replace the real physical product on certainly situation. But it is a still a desire vision currently for most engineer projects.

The design approach based on DMU extended from the CAX and DFX approaches on various professional domains. It combines the progress of some modern techniques such as advanced modeling, advanced simulation, modern information technology and etc.

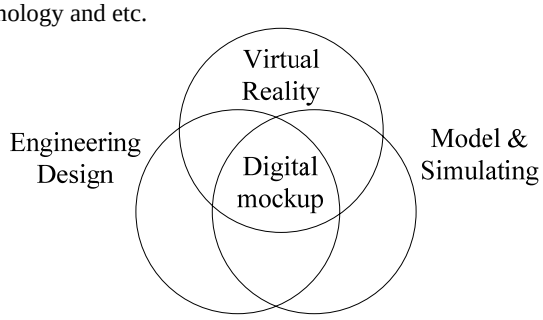

Fig. 1 Techniques supporting DMU

The kernel of DMU is integrated of engineering design techniques, modeling/simulating techniques and virtual reality techniques, show as Fig.1 [1]. The DMU emphasizes the viewpoint of the whole system and entire lifecycle. It supports to evaluate the product property even if the product is not still manufactured.

The design progress based on DMU is certainly unfolded cooperatively among diversified domains [2] [3].

Figure 2 shows how the key supporting techniques sustains constructing the DMU of a product. It indicates that a supporting environment supplies the gap between the virtual prototype and the fundamental supporting techniques [2]. A digital mockup of a complex product has some feathers included:

1) The digital mockup combines of various models such as CAD models, shape model, function model, performance model and environment model etc. These models often are established by different tools in distributed systems;
2) The digital mockup supports product developing over all product lifecycle, includes requirement analysis stage, mental design stage, detail design stage, manufacture/construction stage, test/evaluate stage, maintenance stage and retirement stage etc.
3) The digital mockup involves lots of simulation working in different domains;
4) To establish he digital mockup of a complex product, various objects such as data, models, tools, persons and processes need to be managed orderly.

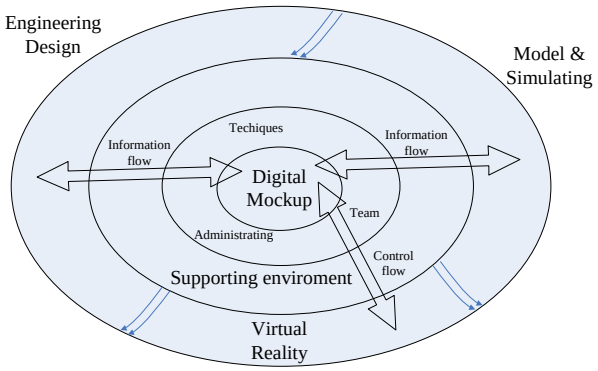

Fig. 2 DMU Applying Frame

The design approach for complex product based on digital mockup needs cooperative working environment natively to supporting the developing process. Such approach needs the cooperative design from multiple professional domains. Before the design is ascertained, the digital mockup of the product is evaluated and modified continuously. Everyone works on the primary DMU, processes information from it and attaches enhance information on it when complete one self's task. Experts need to work on a coherent data source, and should have the ability to associate his working progeny to the DMU, then else could share the benefit of their working effect. The DMU carries the all-round information about a product, but different domain's expert needs a special view of the product. Data often seems necessary for some work, but seems irrespective at the same time for other peoples. Even in some situation, data accessed by some people unreserved would reject some other people rigidly. The supporting cooperative environment keeps the right data always be accessed by the right people at the right time.

This means the product data managed in the environment should not be accessed always if without authorization. Keep the data safe is one of the key goals of the cooperative working environment to support design approach based on DMU.

Product design is iterative processes of requirement ascertain, designing, simulating, evaluating, refers to Fig.3. Design establishes the DMU which meets the requirements as the digital model of the product from blank. The establishment process of DMU comprises of cycle of analysis, design, simulating, evaluating, optimizing, until the design meets the demands. To carry out such a process effectively, a digital cooperative working environment for teams becomes the foundation condition. The basic effect of the cooperative environment represented on the digital model managing, includes below aspects:

1) Centralization manage of product data. In the earlier period of CAD techniques applying, the data of the product often saved in the computer of individuals. Benefits with the information techniques based on networks, the product data of digital model is now saved in a concentration status, or just accessed in a concentration way. The data of product are no longer controlled by the designer directly. This improves the knowledge manageability of the company, and makes the basis of working with mono data source.
2) Versions manage of product data. The design of product always accompanies with series decisions, and change during the design process. The supporting environment must could record the series status of the design model, and track its variance backwardly. Version manage is the basic skill to control the technical status of product data in the supporting environment.
3) Share of the product data. Engineering design is a typical complex cooperative activity. Experts from different department, different professional domain and so on cooperates with each other closely, share the same source product design digital model is a basic demand closely.
4) Access authorization of product data. The demand of data access is not only restricted within the project team. The demand of data access has different types. Sometimes the data should be accessed by someone with some special time. Sometimes only special part of the product design data should be opened for someone. All kinds' data access demand should be controlled by the supporting working environment. It should not block the process of product development, but also makes the data access without authorization being possible.

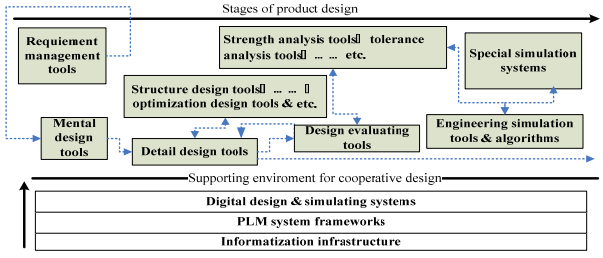

Fig. 3 Digital design process

Access authorization is a basic function of supporting environment for carrying out on digital design. It always realizes from integrating of several techniques and methods. A cooperative working environment is established by the authors to support the design approach based on DMU. Because of the engineer data is the most important knowledge, some enhanced steps is adopted to improve the data security in the system, especially to avoid risk of data accessing without authorization by the administrators.

III. Basic Models of Data Access Control

The goal of data access control is to allow the user with authorization access the related data under special conditions, and avoid the data being accessed without authorization. Lots of cooperative environments set the data access control system based RBDC and its variants. References [6] [7] defined static authorization methods based on the user and his role. Reference [8] defined an authorization method associated process status. Reference [9] defined an authorization model based on datum, workflow, activity, operation and role, and described the modeling process.

A supporting environment for cooperative design managed the product data is established by the authors. The data access control system of which consists some basic techniques described following.

A. Identity authentication

The chiefly demand for access authorization is to distinguish who is requiring the data. Exact user identity authentication is the basis of access authorization. The cooperative system established by the authors identifies users by means of login. People not login will be redirected to the login page. People login in the system has been identified, they access the function of the system under the authorization system.

User/password is a basic identity authentication mechanism. Lots of applications adopt this technique. But in a network environment, this method's limitation is obvious. In the network environment, distinguishing the password is sent by the owner currently has some difficulty. Because the server application could judge the password is right or not, but could not identify password is exactly sent by the owner at the just time. The risk of password leak to a prier always exists. User/password technique is not strong enough for a piratical distributed data manage system. The authors adopt several techniques realized multiple factor authentication; the user could be identified in the system exactly.

B. User management

In the cooperative system, the users with same rights are organized as user groups. Authorization through user groups simplified the control of data access. A certain user group has been authorized to do some special manipulation of the system, then the system could control a user can do something or not edit the relation between the user and the certain user groups. Users in the user groups have the access right. Access right is dropped when the user is dropped off from the user groups.

C.Data information model

In the system data is represented as Fig.4. The origin engineering data are described by various digital files in computer. The computer file corresponds data item in the system. The metadata of data item describes the save location of the computer file in the system. And data item is attached on business item. The system managed product data through the business item. The metadata describes the business item records the attributes of the product data, such as who creates it, when it is created and the last update time and etc [10].

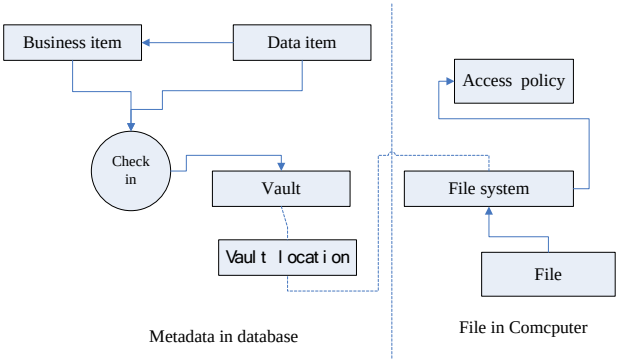

Fig. 4 Data information model

D.Access authorization

An emblematical access authorization system includes factors such as user identity, data distinguishing, acts and conditions. The cooperative system supporting the design approach based on DMU established by the authors adopt a data access control system with the core of message access rule. The rule has structure like Fig.5 [10].

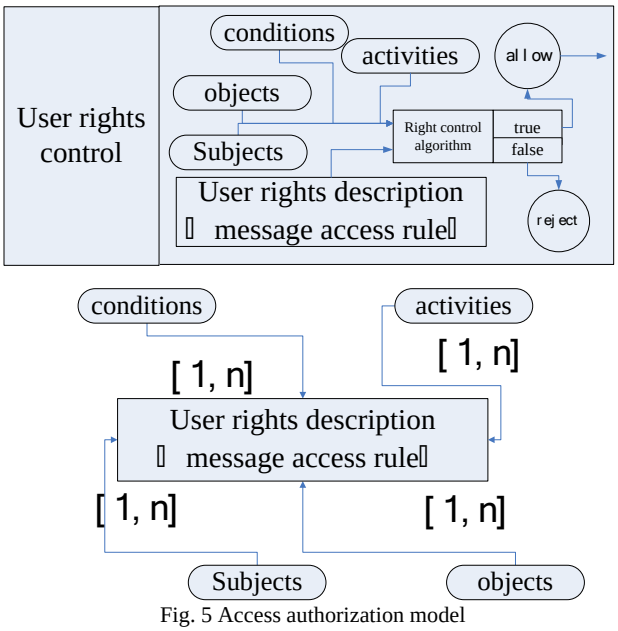

Fig. 5 Access authorization model

In the cooperative supporting environment, business users have been restricted to access data orderly.

1) Participants who can assess the data could be defined clearly in the rule. Participants are managed as a user or user group. Band with the data attributes and manipulate condition, the system could set the authorization just to some user or group user directly or limit the actor by the condition judge.
2) The data could be authorized by its attributes. Band with the condition subsystem, some judgments on data attributes is executed. The return result determined manipulation mentions by the rule could go or not.
3) A process system is adopted in the supporting environment to realize dynamic authorization. The process consists of a series node. Every node has an actor. The actor could do something predefined just within the task period. The actor gets the authorization to access data along with the node task acceptation. The authorization would disappear when the node task is finished.

IV. Deep Demand of Data Access Control

Data access authorization is not only for business users, but also the users who administer the system. But because the administrators often have more privileges to complete their administrating task, the mechanism to prevent them from unauthorized data access is difficult but obligatory. If an administrator pierces into the system and attempt to access data without authorization, the comprehensive intimidate of data leak appears.

Administrators respond obvious task in the system other than the business users. The business users' rights often have been thought over, but on how to prevent administrator access the product data intentionally or unconsciously, the technique way is considered deficiently.

The product data system in a practical cooperative supporting environment is often sensitive and classified. So then even if an administrator, should have no chance to access the data without authorization. Then we must set the system to interdict the latent approaches and prevent administrator access product data optionally out of control.

Some representative risk related administrators includes situations like following descriptions, these all should be processed together.

1) Business user identity imitation. The administrator has the privileges to edit the user's core attribute for login. If some administrators have ability to modify and restore the key login attribute, then the administrator could potentially imitate a business user stealthily, and then get the access authorization entirely of the user.
2) Role adjust by oneself. If the administrator modifies the role of oneself, related one to a special business user group, then the administrator get the all data access authorization upon the user group.
3) Authorization adjustment by oneself. For administrator on duty of authorization, if the administrator could adjust the authorization for oneself directly, then the administrator could give oneself the absolute privilege, and have the potential ability to access any product out of control.

V. Enhanced design of access authorization

In allusion to the risk of data access without formal authorization by the administrators of the cooperative working environment, authors design a set of approaches to prevent the administrator to pierce the system and access the product data optionally. The key principle of the approaches is that anyone could not get excess privileges by oneself. The station role of administrate engenders a mutual restrict situations.

A. Enhanced identity authentication

In the supporting environment, multiple factors have been considered in authentication. The process includes password, USB ekey and fingerprint factors. The dynamic challenge approach is adopted in the login process. Multiple factors authentication improved the login secure strength obviously. The password mechanism prevents aggressor login the system, even if the aggressor gets the user's ekey and make the user provide his fingerprint groggily. And so on, authenticating will pass when the password, the ekey, and the fingerprint are all right. In order to distinguish a user identity through the networks, a mechanism of dynamic challenge and digital signature is adopted. The dynamic challenge makes the record and replay will not affect the login process. The client uses the private ekey sign the challenge from the server, then the server could clearly judge whether the return answer is from the user's key, the user stays at the other end of the cable.

To avoid administrator modify the user's private identity attribute then imitate the user. The right to modify user is separated into two parts, and authorized to different role. Only part of the identity information changes will break the integrity of authentication. Any role of administrator will have no right to modify the user's identity information and imitate the user.

B. Role assign of administrators

Adequate role assign is the key to decrease the risk of administrators to access business data in some informal way. The right of the different administrating role is divided into independent sets. So an entire administrating task would be accomplished cooperatively by two roles at least. Any one of the administrators has no chance to improve self's privileges stealthily.

In the cooperative working environment, the authors provide basic role as follows: administrating role, safety role, rule manage role, audit role. The responsibility of these roles is separated restrictively one by another.

Administrating role has privileges of creating user, modify the user's public key. Administrating role should not have the right to manage the relation of user and user group. Administrating role could not to get unauthorized privileges by creating a new user. Because the user created is not belongs to any user group, the created user has no any rights natively. Obviously, administrating role could not get any informal privileges by creating a new user.

Safety role manages the relation of user and user group for any user except oneself, but who can not create user and modifying the user's public key. Safety role could adjust other's privilege in the system by adding someone into a special user group. But this will not help safety role improve one self's privilege. Rule manage role have the entire rights to adjust anyone's privilege in the system, and could make anyone to do anything. This is a severe menace to data security. A dynamic role assign mechanism is adapted to decrease the risk. The rule manage role has no user assigned on common days. When the rule system needs to adjust, then the safety role assign a user as rule manage role. As soon as the assigned user accomplishes planned work, the relation between user and user group will be dropped immediately. And the activities of the rule manage role user will be audited by an audit role user carefully.

User activities are monitored by audit role. This helps to find out whether if the users use the system as expected.

VI. Conclusion

Cooperative supporting environment is the foundational facility for adopting design approach based on DMU. The data access authorization is a prominent concern in such working environment over the whole enterprise. Business user has been controlled rigidly in common other than the administrators of the working environment. Enhanced system has been established to restrict data access for users include administrators. Restricted by such a system, administrators no longer have the chance to improve their privileges stealthily to access data without informal authorization. The security of engineering data, the knowledge belongs to the enterprise is enhanced effectively due to this system and some other matching measures.

Acknowledgment

Relate work was financially supported by the Technology Development Fund of China Academy of Engineering Physics (2009A0203011).

References

[1] Xiong Guangleng, LI Bohu, Chai Xudong, "Virtual Prototyping Technology". Acta Simulata Systematica Sinica, vol.13, no.1, pp. 114–117, 2001.

[2] Ting Huang, C.W. Kong, H.L. Guo, Andrew Baldwin,Heng Li, "A virtual prototyping system for simulating construction processes", Automation in Construction, vol.16 , pp576-585, 2007.

[3] Qing Shen, Michael Grafe, "To support multidisciplinary communication in VR-based virtual prototyping of mechatronic systems, Advanced Engineering Informatics", vol.21, pp201-209, 2007 .

[4] Li Bohu, Chai Xudong and etc., "Research and Practice on Complex Products Virtual Prototype Technology", Measurement & Control Technology, vol.20, no.11, pp. 1–6, 2001.

[5] Li Bohu, Chai Xudong, "Virtual Prototyping Engineering for Complex Product ", Computer Intergratated Manufacturing Systems, vol.8, no.9, pp. 678–683, 2002.

[6] Sandhu R., "Role-based access control", Advances in Computers, vol.1, pp46-49, 1998.

[7] Zhu Hong, Feng Yucai, Wu Yongying, "Secure Administration Based on User Role", JOURNAL OF HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY, vol.28, no.4, pp23-25, 2000.

[8] Gou Jihua, Peng Yinhong, Ruan Xueyu, "Modeling technique of PDM implement", CAD/CAM, vol.6, pp12-15, 1999.

[9] Zhou Yanfei, Ma Ben, Wang Linbo, Yuan Puji, "User Access Control Modeling for PDM Systems", Journal of Data Acquisition & Processing, vol.4, no.12, pp385-389, 2002.

[10] Wei Lifan, Zhang Haiyu, Jia Li, "A Bussiness Intergration Model Used In Collaborative Engineering Design", in 2011 International Conference on Advanced Design and Manufacturing Engineering, GuangZhou, pp162-166.