COMPUTER-AIDED DESIGN & APPLICATIONS, 2016
VOL. 13, NO. 3, 397–408
http://dx.doi.org/10.1080/16864360.2015.1114398

Hierarchical Role-Based Access Control for Multi-User Collaborative CAD Environment

Chia-Chi Teng, Francis N. Mensah, J. Ekstrom, Richard Helps and C. Greg Jensen

Brigham Young University

ABSTRACT

Commercial computer aided design (CAD) applications have traditionally been based on a single user architecture. Recent research on multi-user collaborative CAD and other computer aided applications (CAx) have shown promising and highly functional prototypes of multi-user concurrent designing tools based on popular and market leading commercial software systems such as Siemens NX. However, for these prototypes to be deployed to the real-world corporate environment for commercial projects, security features such as access control and encrypted transport must be implemented as integral part of the enterprise network infrastructure.

Directory services (DS) such as Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP) has become the standard software and protocol for managing resources in the complex modern enterprise network. DS controller authenticates and authorizes user's access to resources and enforces security policies. This research presents a method to integrate existing corporate DS and user information to provide a role-based access control functionality in multi-user CAD software. A successful prototype system was built based on previously published multi-user enabled Siemens NX CAD software and integrated with a Microsoft Active Directory domain services where users and roles where created to simulate a corporate engineering organization. The system was then validated with models and assemblies where components were configured with various access privileges.

KEYWORDS

Multi-user CAD; Collaborative Design; Access Control; Security

1. Introduction

While the engineering design and manufacturing are highly collaborative processes, main stream commercial CAD and other computer-aided tools still limited to user interface and user experience that are single user in nature. The collection of single user tools unnecessarily constraint the design and manufacturing processes with too much serialization or difficult integration when teams of engineers are involved in complex projects. The lack of concurrent and distributed CAx tools not only limits the productivity and efficiency of the engineers, but also create risk in quality management in today's increasingly complex systems, which in turn lengthens the product development life cycle and increases cost.

Researchers have proposed a variety of methods and tools to facilitate concurrent multi-user collaboration in CAD modeling [20], mostly notably the NX-Connect system built by the National Science Foundation (NSF) Center of e-Design [3] at Brigham Young University who successfully integrated such capability in the one of the world leading commercial CAD application – Siemens NX [15]. The NX-Connect system is designed to support engineering teams that are distributed in multiple geographical locations connected through public internet infrastructure [21]. Past experimental design projects involving engineering students from multiple universities across the country have demonstrated the feasibility of such collaborative design process and the potential productivity gain [22].

But for such tools to be introduced to the real world commercial product design and development, they need to address and comply with a long list of security requirements that are essential in the complicated corporate organization and enterprise network environment. The primary research objective of this paper is to design a security abstract layer that can be integrated with multi-user collaborative computer-aided engineering tools that can properly authenticate users and authorize proper access rights to hierarchy of objects based on the users' roles and access privileges in the organization. In order to validate the concept and create a functional prototype, such a security framework was built, integrated and tested with the current NX-Connect system.

CONTACT Chia-Chi Teng ccteng@byu.edu

2. Background

2.1. Collaborative CAx

The potential benefit and motivation for more collaborative computer software have been well addressed in the literature [2]. There have been ample research activity dedicated in the past decade to methods and tools for collaborative engineering design [9],[20], including the v-CAx and NX-Connect projects [11] at the NSF Center of e-Design [3],[10],[16,17]. These studies have shown great potential benefits both in cost and performance from collaborative CAD and other engineering design tools. There is also active participation from the industry with great interests to see actual deployment of these collaborative tools in their global training and production environment [18],[22].

In addition to the v-CAx project, there are a number of other research groups who have also developed multi-user collaborative modeling and design tools that demonstrated feasibility and practical use. For instance, MUG [4], CADDAC [14], e-Assembly [6], WebSpiff [1] and WPDSS [12]. Although the current state of many multi-user CAD prototypes, including NX-Connect, is highly functional with most of the features needed to execute concurrent design of complex engineering models, they do not have sufficient security measures for them to be deployed in commercial project where protection of intellectual property is essential. For example, the communication between clients and servers are not encrypted and all users have rights to access all objects in the assembly and parts. In order for the multi-user systems to be successful in the real world application, it must include up-to-date security protocols such as secure transport and access control suited for the target organizations.

Even though the ability to manage user permission has been available in commercial PLM systems for a number of years, for example, both Siemens' Teamcenter [13] and Dassault System's ENOVIA [7] software have features allowing users to control various security settings and access privileges. There are still many limitation and shortcoming with the way they are currently implemented in both of these market leading systems.

First, these software manage their user credential and permissions as independent and standalone systems that are not integrated with the corporate directory services. User information in the corporate directory services are not easily transferrable to the PLM system, and vice versa. Maintaining two separate user and resource management systems not only require addition men-hour but also often leads to administrative errors or data being out of sync.

Second, even though Teamcenter and ENOVIA systems supports access control to CAD parts and assemblies, they do not allow multiple users to access or edit a part at the same time. For a multiuser CAD system to be truly collaborative, it needs to allow concurrent access to CAD models from any number of users so long as their privilege are enforced. For example, a CAD part can be edited by multiple engineers working on the design, and view by others with read-only access.

Third, the granularity of the access control in the Teamcenter and ENOVIA systems are limited at the part or file level. The NX Connect system has the ability to support access control at the sub-part or feature level, which can potentially provide greater flexibility for more effective project management.

Figure 1 shows the architecture of the previous NX-Connect system prototype where a simple username/password authentication is taken place against a local and isolated database. In addition, the data streams between clients and server were not encrypted. The system as it was could not be used in commercial engineering development simply because the lack of security protocol.

2.2. Security Risks

As the CAD software and other CAx tools transition from a single user application to a multi-user concurrent collaborative system operating in a geographically distributed network environment, they can be exposed to many security threats. For examples,

- Unauthorized access to system and resources
- Unauthorized user operation
- Server identity theft
- Eavesdropping or sniffing

For the traditional single-user applications, the workstation operating system typically authenticate users through corporate network directory service and credential, where logging in to the workstation typically grant access to the CAD/CAx software and data files. In a multi-user environment where shared modeling and design data reside on the network servers, access request from client applications will require network authentication protocol. In addition, it is also possible for an attacker to take on the identity of an authentic server and have users unknowingly communicating with a fake server rather than the authentic one, where sensitive design data can be made available to an unauthorized party.

As authorized users gain access to the system, they should only be able to have access to and perform operations on data which they are permitted to. Without role-based access control, shared classified data can be inadvertently destroyed, intentionally stolen or

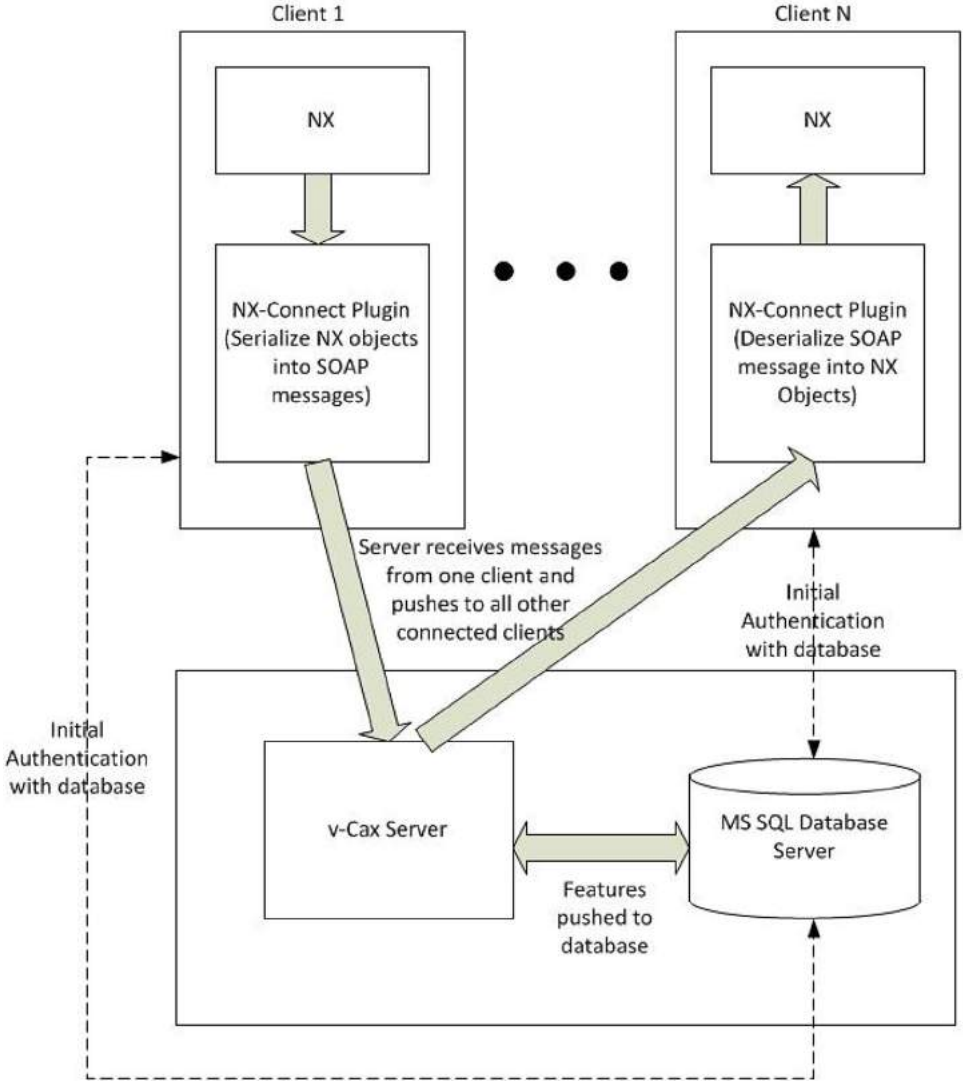

Client 1
NX
NX-Connect Plugin (Serialize NX objects into SOAP messages)
Client N
NX
NX-Connect Plugin (Deserialize SOAP message into NX Objects)
Server receives messages from one client and pushes to all other connected clients
Initial Authentication with database
Initial Authentication with database
v-Cax Server
MS SQL Database Server
Features pushed to database

Figure 1. Original design of NX-Connect with simple database authentication and no encryption.

sabotaged. Furthermore, communication carried over networks can be sniffed or captured using various network capture tools. Design data sent back and forth between clients and servers can be intercepted if they were not property encrypted. The exposure of a multiuser CAD system to any of these threats can result in some devastating consequences and thus steps need to be taken to minimize the risks and mitigate the effects of such vulnerabilities.

2.3. Security Requirements

Few references are found in literature that focused on the security aspect of multi-user collaborative CAx, even though protection of information from malicious activities or unintentional errors is a crucial part of any engineering development environment. A study by Zhang et al reviewed some of the security requirement in a collaborative system and how they might relate to the general information technology (IT) systems, including some discussion of access control pertaining to CAD models [23], wherein a layered approach was suggested. The three security layers and their primary functions were identified as the following:

- Data and communication layer: ensure confidentiality and data integrity
- Access control layer: manage authentication and authorization
- Collaborative process layer: coordinate activities in the design process

The work of this research and the discussion below will primarily focus on the data communication and access control layers.

The most common mechanism for ensuring confidentiality is encryption with symmetric or asymmetric algorithms such as, but not limited to, DES (Data Encryption Standard), AES (Advanced Encryption Standard), RC4 (Rivest Cipher 4) or RSA (Rivest-Shamir-Adleman). Standard encryption protocols have been developed based on these algorithms to support secured network communication, for examples, Transport Layer Security (TLS) and Internet Protocol Security (IPSec). Integrity provide assurances that data received from the network transmission has not be modified and the data is from the sender as it is claimed. Cryptographic hashing and digital signatures are two most commonly mechanisms for maintaining data integrity. Research by Rouibah and Ould-Ali demonstrated the use of TLS and digital signature in a prototype of collaborative product definition management system [19].

Authentication and Authorization are two processes that usually complement one another. While authentication ensures that only legitimate users have access to a system, authorization manages the rights of the users after they have been granted access to the system. Protocols such as Kerberos and TLS are regularly used in conjunction with directory services and digital certificates such as X.500 and X.509 to manage authentication in today's enterprise network environment where mutual authentication is typically required between the server and client. Implementation and support of these standard protocols can be found in popular commercial network management systems such Microsoft Windows Server which includes directory services that manage security and identity information pertaining to an organization's network resources and users. Most directories follow a hierarchical format based on the X.500 standard and access protocols such as Lightweight Directory Access Protocol (LDAP) that allows users and applications to interact with the directory.

In addition to authentication, the access control layer is also responsible for authorization, thus ensuring that only authorized users can access specific CAD model parts and assemblies. The most commonly used access control models in practice are Discretionary, Mandatory and Role-based, where each of them have their strengths and weaknesses, some hybrid implementation have, over time, been developed and adopted in various software systems.

2.4. Role-based Access Control

In computer science, an access control matrix is an abstract and formal security model of information protection in computer systems that characterizes the rights of users with respect to objects in the system. Role-based access control (RBAC) and mandatory access control (MAC) are two commonly used mechanisms in modern operating systems to manage user access to files, network ports or other objects [8]. Even though it was not specifically mentioned in their paper, Cera et al. applied the concept of hybrid access control in a technique called Role-based Viewing for collaborative 3D geometric model design [5], where a variable level-of-detail meshes is created across both individual parts and assemblies to provide a model based on the access rights of the individual actors within a collaborative design environment. This result is achieved through an integration of RBAC and Bell-La Padula model which is an implementation of MAC.

Hierarchical role-based access control is a variant of RBAC that incorporates inheritance of attributes in a hierarchy of objects, which is also often used in complex software systems. For the scenario of multi-user CAD design, a similar access control matrix can be defined based on the organizational need of the engineering team. Various access rights to certain hierarchy of objects in the assemblies or parts can be given to selective roles and privileges of users. We propose a design that combines both RBAC and MAC which can be integrated with multi-user CAD or other computer-aided applications to satisfy the need of a real-world enterprise level concurrent collaborative tool.

Any large scale engineering organization typically uses a directory service to manage hierarchies of users and resources. Most such services have standardized on an open and vendor-neutral industry standard known as LDAP. To effectively integrate a multi-user collaborative tool into the enterprise environment, it is imperative that one must incorporate an access control function that is compatible with an LDAP service.

3. Method

To demonstrate the design and functionality of the new security features in a multi-user CAD system, we used the NX-Connect system prototype (Fig. 1) as the base whereon the security layers were added to manage access control and secured communication through integration with enterprise directory services. A simulated corporate environment is setup with network domain controllers and services where user credentials and security objects can be defined as they would be in a real world engineering projects. Although implementation and support of the standard security protocols can be found in most popular commercial network management systems, we chose Microsoft Windows Server platform for our reference design because of its dominant market share and easy to use programming interface. In addition, the schema and data source for the collaborative model with hierarchies of assemblies and parts need to be extended to

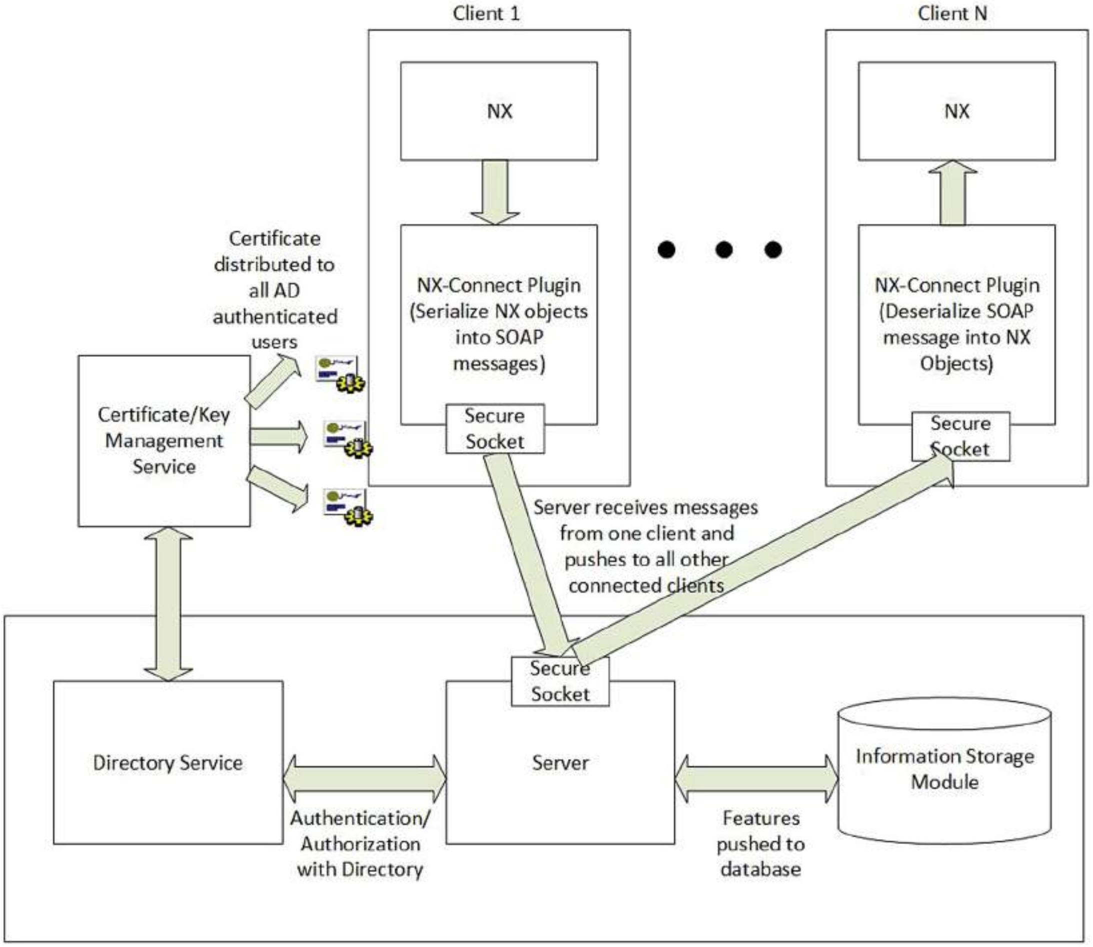

Client 1
Client N
NX
NX
NX-Connect Plugin (Serialize NX objects into SOAP messages)
NX-Connect Plugin (Deserialize SOAP message into NX Objects)
Secure Socket
Secure Socket
Certificate distributed to all AD authenticated users
Certificate/Key Management Service
Server receives messages from one client and pushes to all other connected clients
Secure Socket
Directory Service
Server
Information Storage Module
Authentication/ Authorization with Directory
Features pushed to database

Figure 2. Proposed new system with: (1) authentication with directory service, (2) encrypted data stream, (3) RBAC and MAC for objects in the model assembly.

include access control permission attributes as defined in the directory services.

Comparing to the previous prototype of NX-Connect, Fig. 2 shows the revised system overview diagram with the addition components, i.e. directory and certificate management services, and added security layers in existing client and server components. Details of these new software modules will be discussed below.

3.1. Authentication

When a user starts a new session of NX-Connect multi-user CAD application on a client workstation, the request to access the NX-Connect server will now prompt user to enter his network domain credential which will be validated through encrypted channel with the domain directory server as shown in Fig. 3. This new layer of security protocols for secured authentication are added to the NX-Connect plug-in on the client workstation and the NX-Connect server to fully integrate the user authentication process with the corporate network.

3.2. Authorization

After a user is authenticated, a hybrid authorization model consist of MAC and RBAC is adopted in the design to support the typical organizational need for both commercial and classified engineering projects. The following concepts are used to formalize the authorization process when a user requests access to a particular set of data, e.g. a part or assembly.

3.2.1. Security class

The security class of a subject or object determines sensitivity levels. In order for a subject (user) to have access to an object (CAD model), the subject must have a security class that is higher or equal to the security class of the object. Security classes follow a hierarchical structure. This means that security classes have associated levels with one level trusted more than the other. For example, in a government contracted project, security classes may include unclassified, confidential, secret and top secret, with increasing levels in that order.

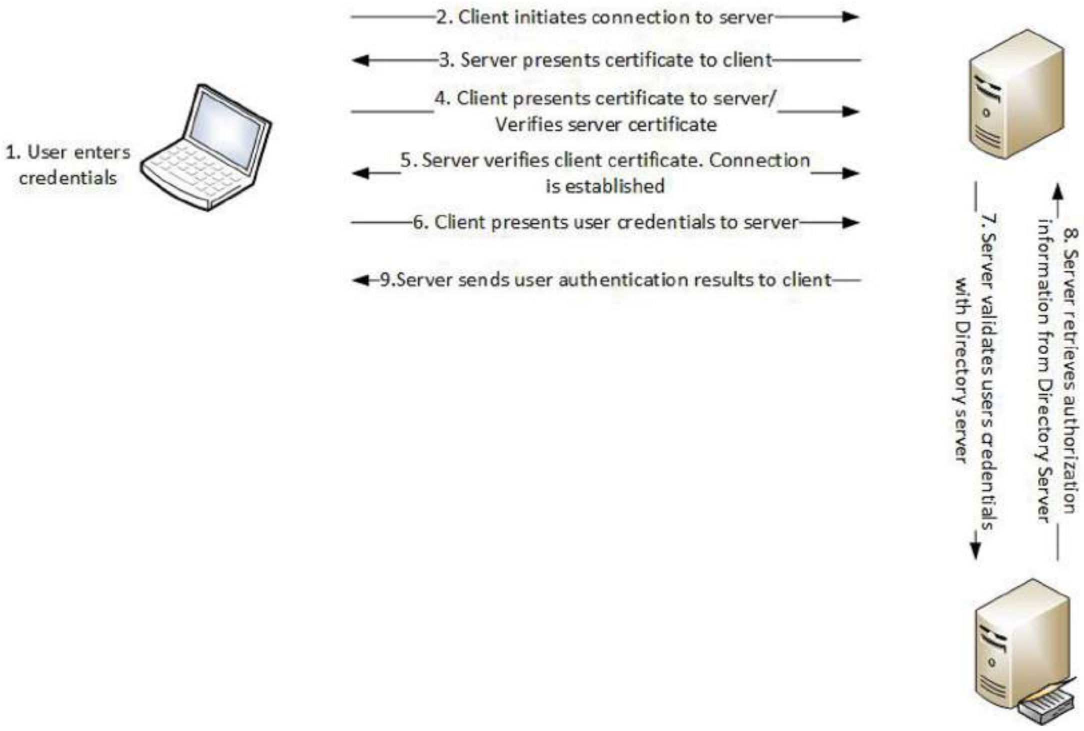

1. User enters credentials
2. Client initiates connection to server
3. Server presents certificate to client
4. Client presents certificate to server/ Verifies server certificate
5. Server verifies client certificate. Connection is established
6. Client presents user credentials to server
7. Server validates users credentials with Directory server
8. Server retrieves authorization information from Directory Server
9.Server sends user authentication results to client

Figure 3. User authentication process.

3.2.2. Security category

Security categories enforce need to know rules. The fact that user A, for example, has a certain security clearance (security class) does not guarantee access to a CAD model, even if that CAD model also belongs to that security class. User A must also belong to the security category of the CAD model data in question. Security categories do not follow a hierarchical structure like security classes, and may be based on projects, geographic locations or other factors.

3.2.3. Role

Rather than assigning permissions on objects to individual users, a role can be created to which a user may be assigned. This simplifies the process of granting permissions. Granting permissions to roles is a feature of RBAC. The design of RBAC in the framework is hierarchical, which means that there is an accumulation of permissions of other roles or in other words privilege inheritance. For example, a Technician role may have certain permissions and the Junior Engineer role also has its permissions. A Senior Engineer Role inherits the permissions of the two roles in addition to other permissions assigned to the Senior Engineer role.

3.2.4. Authorization process

Each user is assigned a label comprising a security class and security categories which must match that of a CAD model's label before the user is granted access to that object (part or assembly). After a user has been granted access to a part, the user's roles determine the operations that can be performed on the CAD model. Such actions may include viewing, modifying, deleting, or creating an object. The permissions that are assigned to roles can fall under two categories: global permissions and object permissions. Global permissions apply to all CAD models in a specific database. Object permissions on the other hand apply only to specific objects. For example, a global permission "View" means that a user has permission to view any CAD model. An object permission "Delete" for the CAD model "Part-A" means that the "Delete" operation can only be performed on Part-A. Fig. 4 illustrates the authorization process described above. These access control functionalities require changes in the data management structure which will be address later.

3.3. Network Domain Services

Typical enterprise network infrastructures rely on some form of directory service to manage the users and resources. Most of these directories follow a hierarchical database format based on the X.500 standard and implements protocols such as LDAP to interface with users and applications. Based on the suggestion from our industry partners, we chose to use Microsoft Active Directory in our reference design. A separate GUI management

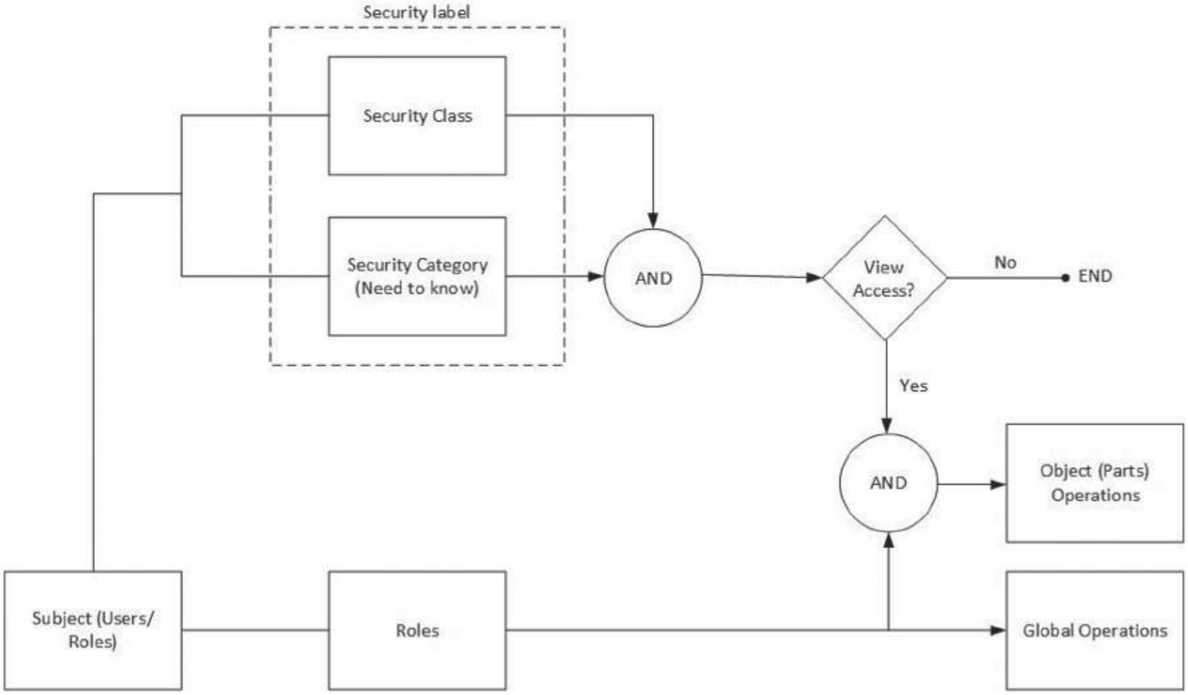


Figure 4. Authorization process.

console tool was developed to create and manage security classes, security categories, user roles and permissions in the directory through application programming interface (API). These security objects are made available through the directory service and used by the new access control layer in the NX-Connect system, as shown in Fig. 2.

For the data communication security layer, the standard TLS protocol was adopted not only to encrypt the network transmission channel, but also to mutually authenticate the identities of client and server through the use of digital certificates or public key infrastructure (PKI) to prevent spoofing and other similar attacks. The certificate authority (CA) is one of the main features of PKI which is a trusted third party (other than the client and server) that manages and issues digital certificates. A detailed description of PKI is not in the scope of this manuscript, suffice to say that it is commonly used as part of any enterprise network security protocol and a well-managed PKI service is a crucial component to a secured network environment, especially when multiple geographically dispersed locations are involved and proprietary data being transported through public network infrastructure. This reference design leverages the Certificate Services on Microsoft Windows Server which seamlessly integrate with the Microsoft Active Directory and network domain controller to provide digital signatures and certificates to ensure the chain of trust. The certificate/key management service component shown in Fig. 2 interacts with client workstations and servers to facilitate cross authentication and secured transport through proper distribution of certificates/keys.

3.4. NX-Connect Clients

A data communication security layer is added to the NX-Connect clients to perform the following functions:

- **DOMAIN AUTHENTICATION**. Instead of operating with a different set of login credential, the system will now require users to login with the same user credential for accessing other corporate network resources and authenticate through the domain directory services. By integrating with the corporate directory service, the system will have access to up-to-date user information for proper authentication. This also enables the system to link users to security objects to support RBAC and MAC on the data objects later on.
- **SECURED TRANSPORT LAYER**. After the user is authenticated, proper digital signature or certificates are given to the clients (and server) from the certificate management services to encrypt their communication channel with TLS, an industry standard secure communication protocol.

3.5. NX-Connect Servers

The NX-Connect servers encompasses two main components: 1) the data management component that manages the database of CAD models, 2) the NX-Connect servers that manages the communication with clients and authorization of resources. Added security functions for each of the components will be discussed below.

3.5.1. Database server

The object classes in the database are structured to represent information for typical CAD models, including assemblies and parts with their geometric and other features. These object classes need to be modified or extended to include access control information including user roles and security class that are allow for various actions (create, view, modify or delete). Fig. 5 shows a partial view of the new schema which now include tables of access permission information.

3.5.2. NX-Connect server

This is the communication and mediation layer between the client applications and the database server. First of all, it now uses the domain authentication and certification services to coordinate secure communication with the clients. Secondly, after a user is authenticated, it now works with the Active Directory server to enforce RBAC and MAC and authorize or deny user request to access data objects in the model based on the authorization process described in earlier sections. Only users with proper role and security privilege are granted access or action to the data object. Hierarchical inheritance of security attributes in the CAD model can also be enforced here. Fig. 2 illustrates the new architecture and how all the components interact with each other.

4. Results

A functional prototype was successfully built and validated with a simple simulated engineering organization which contains multiple roles of engineers and levels of security privileges. A small set of simple CAD assemblies each containing multiple parts and various permission settings were built with this new system to mimic real world applications. The system was tested with multiple users/clients with different roles and privileges who work in concurrent sessions connecting to the server through domain authentication while working on the same model. A set of scenarios were executed to validate the security and access control requirement.

The development and testing environment is built on a VMWare ESXi virtual machine (VM) environment to simulate real world corporate network infrastructures. Various server VMs and multiple client workstation VMs were setup and configured to represent different components in the NX-Connect system as shown in Fig. 6. All servers run on Microsoft Windows Server 2012 even though they act in different capacities. Client workstations run Windows 7 and the latest NX-Connect CAD software. All security functions and interaction with the domain services are implemented with Microsoft .NET Framework APIs and Microsoft Windows Server SDK.

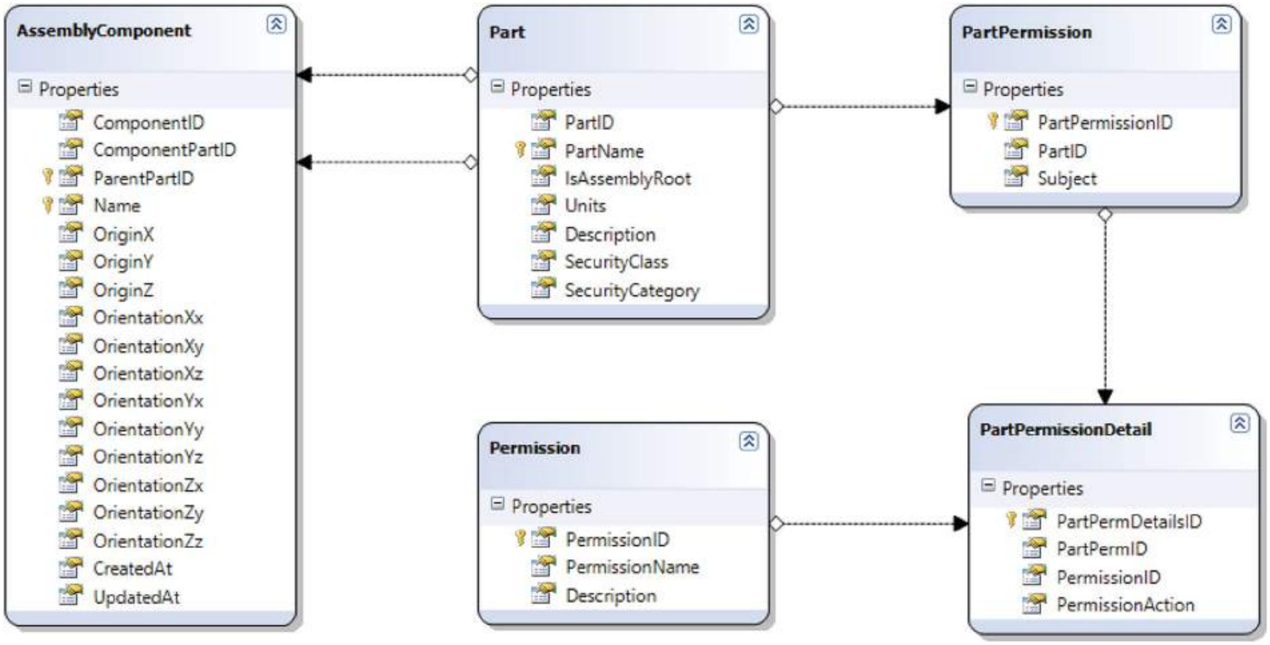


Figure 5. Schema extension for access control.

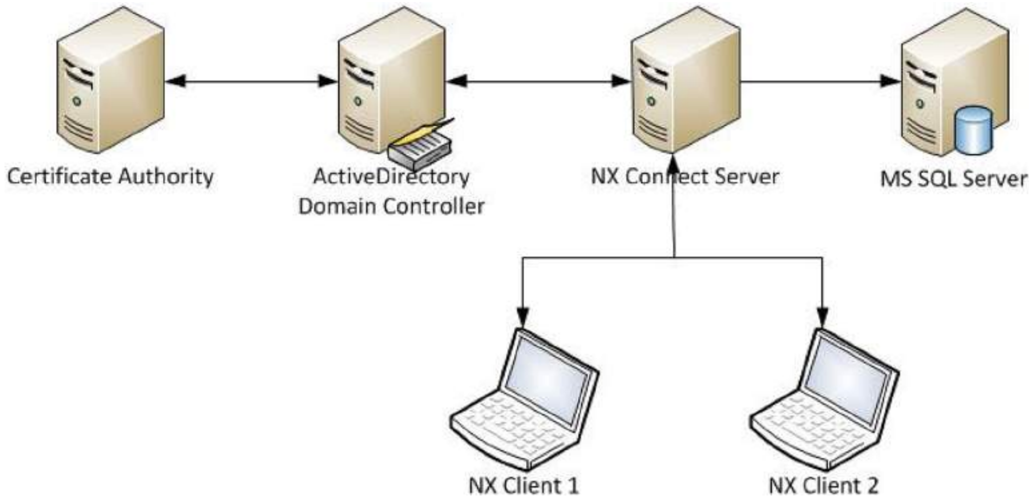
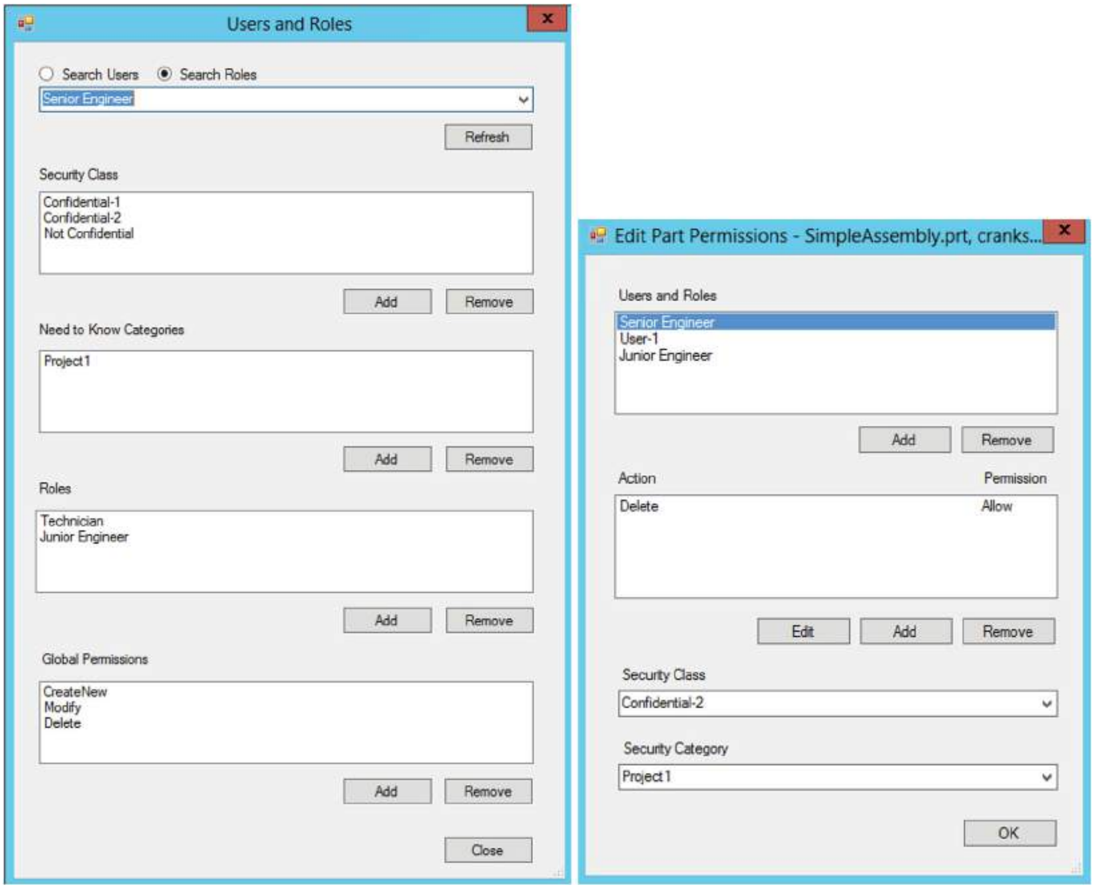


Figure 6. Server topology diagram.


Users and Roles

○ Search Users ● Search Roles

Senior Engineer

Security Class

Confidential-1
Confidential-2
Not Confidential

Need to Know Categories

Project1

Roles

Technician
Junior Engineer

Global Permissions

CreateNew
Modify
Delete

Edit Part Permissions - SimpleAssembly.prt, cranks...

Users and Roles

Senior Engineer
User-1
Junior Engineer

Action	Permission
Delete	Allow

Security Class: Confidential-2

Security Category: Project1

Figure 7. Screenshots of GUI management console for access control settings. Left (a) shows UI for user permissions and right (b) shows UI for object permissions.

In the simulated engineering organization, a number of users were conceptualized with various roles and security permissions. After basic user credentials are setup in the Active Directory, security objects are created and managed with a GUI management console developed in C# programming language. Fig. 7 includes screenshots of the GUI management console where 7(a) shows a senior engineer inheriting security settings under his hierarchy

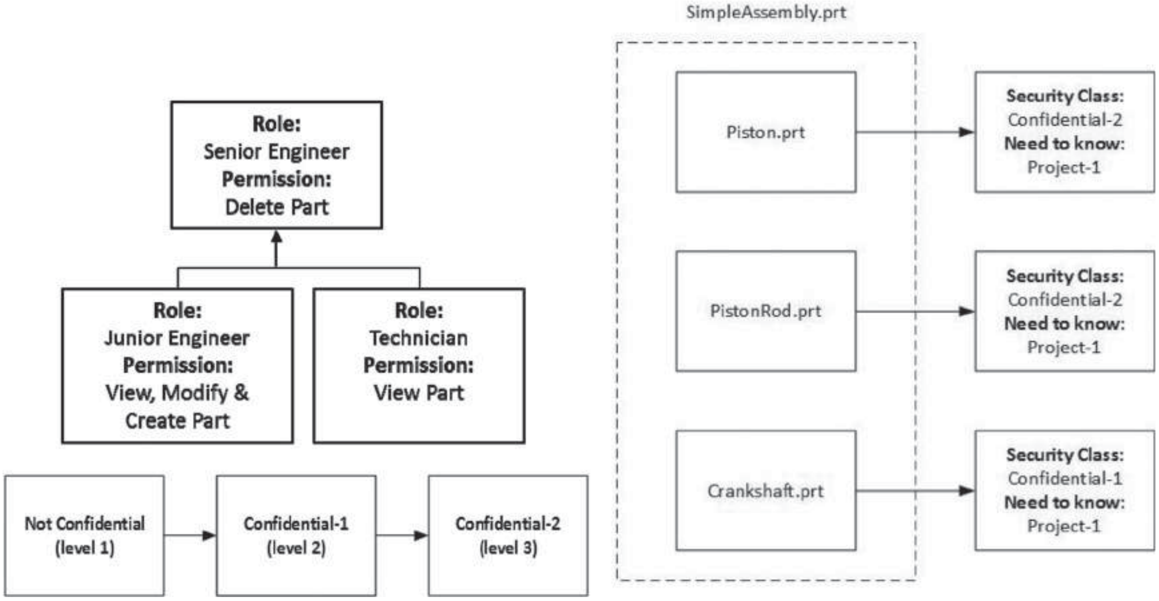


Figure 8. Sample test case. Left (a) shows the roles and security classes and right (b) shows the object permission in the CAD model.

Table 1. User security settings in directory service.

	Security Class	Need to Know	Roles
User-1	Confidential-2	Project-1	Sr. Engineer
User-2	Confidential-1	Project-1	Technician

of roles who is also associated with other mandatory security attributes; and 7(b) shows the permission setting of a part in the CAD model.

A small number of test cases with a metric of scenarios were developed to validate the functionalities according to the requirements. Fig. 8 shows one such test case where 8(a) consists of an organization with a hierarchy of three roles and three level of confidentiality, 8(b) represent a simple assembly containing three parts each with different permissions. Tab. 1 defines two users in the organization with different security settings. Three simple test scenarios will be described below.

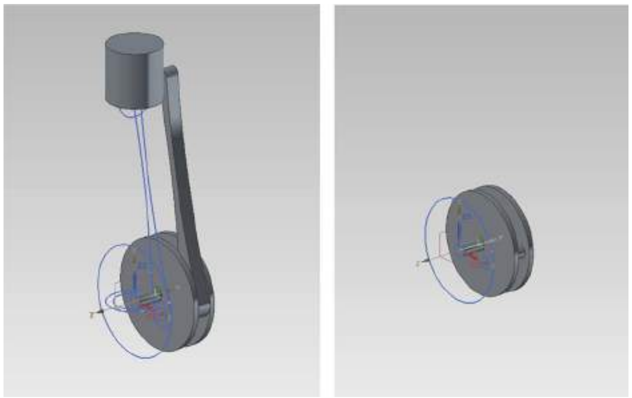


Figure 9. Test scenario 1. Left, screenshot of User-1′s view in NX client. Right, User-2.

4.1. Scenario 1

With the configuration and permissions shown in Fig. 8 and Tab. 1, the two users start a new working session on two separate client workstations. User-1, as a Sr. Engineer and Confidential-2 security class, can view all the three parts in the assembly. However, User-2, because of his Confidential-1 security class, can only see the crankshaft part, as shown in Fig. 9.

4.2. Scenario 2

We then modify the security class of the piston rod to Confidential-1, User-2 will now able to view the piston rod, but still not the piston. Screenshots shown in Fig. 10.

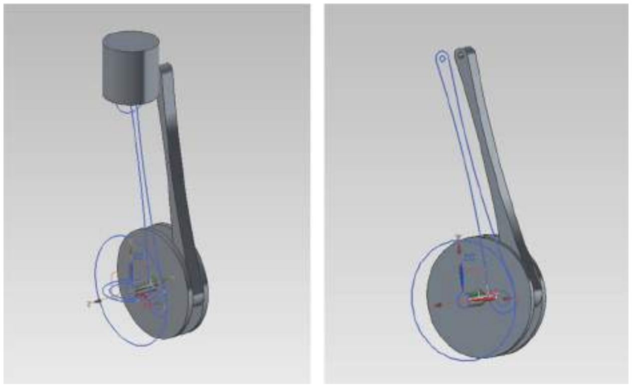
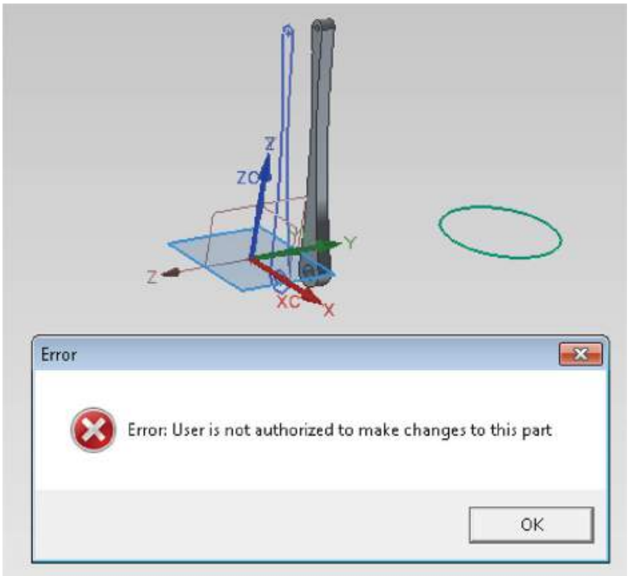


Figure 10. Test scenario 2. Left, screenshot of User-1′s view in NX client. Right, User-2.

4.3. Scenario 3

In Fig. 8(a), the Senior Engineer only is shown with only one permission setting for deleting parts. However, because it inherits Junior Engineer and Technician in the hierarchy, a Senior Engineer can view, modify and create parts without having to explicitly assign the permissions. As shown in earlier scenarios, User-1 can view all the parts in the assembly. In addition, when User-2 attempts to modify the piston rod, an error will occur in the authorization layer because of mismatched permissions, as shown in Fig. 11.



Error: User is not authorized to make changes to this part

Figure 11. Screenshot of User-2's NX client when attempting to modify the piston rod.

5. Conclusion

This paper proposed a design to address the compelling need of security protocols in the current state of the art multi-user concurrent collaborative engineering tools. As multi-user CAD become closer to being commercially viable, security concerns will need to be addressed prior to being deployed to an enterprise environment. Role-based and mandatory access control integrated with standard enterprise network services is a practical and effective approach that can provide sufficient functionality for common security requirements. The resulting prototype may have certain limitations and requires more stringent testing, however, the new and improved NX-Connect with built-in RBAC and MAC has shown that multi-user CAD system with sufficient security features can be a reality in real-world complex commercial engineering projects in not so distant future.

Acknowledgement

The authors would like to thank the NSF and Center of e-Design members for their funding and support for the research projects at BYU.

ORCID

Chia-Chi Teng http://orcid.org/0000-0001-9101-056X
C. Greg Jensen http://orcid.org/0000-0003-1824-0945

References

[1] Bidarra, R.; van den Berg E.; Bronsvoort W. F.: A Collaborative Feature Modeling System, Journal of Computing and Information Science in Engineering, 2(3), 2003, 192–198. http://dx.doi.org/10.1115/1.1521435

[2] Bouras, C.; Giannaka E.; Tsiatsos T.: E-Collaboration Concepts, Systems and Applications, E-Collaboration: Concepts, Methodologies, Tools and Applications, Information Science Reference, Hershey, NY, 2009.

[3] Center for e-Design, http://centerforedesign.org, National Science Foundation.

[4] Cera, C. D.; Regli W. C.; Braude I.; Shapirstein Y.; Foster C. V.: A Collaborative 3D Environment for Authoring Design Semantics, IEEE Computer Graphics and Applications, 22(3), 2002, 43–55. http://dx.doi.org/10.1109/MCG.2002.999787

[5] Cera, C. D.; Braude, I.; Kim, T.; Han, J.; Regli W. C.: Hierarchical Role-Based Viewing for Multilevel Information Security in Collaborative CAD, Journal of Computing and Information Science in Engineering, 6(1), 2005, 2–10. http://dx.doi.org/10.1115/1.2161226.

[6] Chen, L.; Song Z.; Feng L.: Internet-Enabled Real-Time Collaborative Assembly Modeling via an E-Assembly System: Status and Promise, Computer-Aided Design 36(9), 2004 835–847. http://dx.doi.org/10.1016/j.cad.2003.09.010

[7] He, Y.; Zhang, W.; Xie J.; Wang, J.; Qiu, H.: Intgegrated Application of PLM based ENOVIA Platform in Domestic Manufacturing Industry, International Conference on Information Management, Innovation Management and Industrial Engineering, 2011, 226–229. http://dx.doi.org/10.1109/iciii.2011.202

[8] Kim, S.; Kim, D.-K.; Lu, L.; Park, S.; Kim, S.: A Feature-Based Modeling Approach for Building Hybrid Access Control Systems, Fifth International Conference on Secure Software Integration and Reliability Improvement, 2011, 88–97. http://dx.doi.org/10.1109/SSIRI.2011.16

[9] Li, W. D.; Lu W. F.; Fuh J. Y. H.; Wong Y. S.: Collaborative Computer-Aided Design—research and Development Status, Computer-Aided Design, 37(9), 2005, 931–940. http://dx.doi.org/10.1016/j.cad.2004.09.020

[10] Moncur, R; Jensen, C. G.; Teng, C.-C.; Red, E.: Data Consistency and Conflict Avoidance in a Multi-User CAx Environment, Computer-Aided Design & Applications, 10(5), 2013, 727–744. http://dx.doi.org/10.3722/cadaps.2013.727-744

[11] New Multi-User Computer-Aided Applications, http://v-cax.byu.edu, Brigham Young University.

[12] Qiang, L.; Zhang Y. F.; Nee a. Y. C.: A Distributive and Collaborative Concurrent Product Design System through the WWW/Internet, International Journal of Advanced Manufacturing Technology, 17(5), 2001, 315–22. http://dx.doi.org/10.1007/s001700170165

[13] Pokale, S. B.; Borul, S. S.; Rodge, M. K.: Client Side Customization for Checking User Rights in Teamcenter-PLM, International Journal of Applied Information Systems, 5(10), 2013, 9–14. http://dx.doi.org/10.5120/ijais13-450975

[14] Ramani, K.; Agrawal A.; Babu M.; Hoffman C.: CADDAC: Multi-Client Collaborative Shape Design System with Server-Based Geometry Kernel, Journal of Computing and Information Science in Engineering, 3(2), 2003, 170–173. http://dx.doi.org/10.1115/1.1582882

[15] Red, E.; Jensen, C. G.; Ryskamp, J.; Mix, K.: NXConnect: Multi-User CAx on a Commercial Engineering Software Application, PACE Glob Annu Forum, 2010, 1–9.

[16] Red, E.; Holyoak, V.; Jensen, C. G.; Marshall, F.; Ryskamp, J.; Xu, Yue.: v-CAx: A Research Agenda for Collaborative Computer-Aided Applications, Computer-Aided Design & Applications, 7(3), 2010, 387–404. http://dx.doi.org/10.3722/cadaps.2010.387-404

[17] Red, E.; French, D.; Jensen, C. G.; Walker, S. S.; Madsen, P.: 2013. Emerging Design Methods and Tools in Collaborative Product Development, Journal of Computing and Information Science in Engineering, 13(3), 2013. http://dx.doi.org/10.1115/1.4023917

[18] Richey M.; Zender F.; Schrage D.; Jensen C. G; Fehr J.; Symmonds M. M.; French D. E.; McPherson B.; An Innovative Approach to an Integrated Design and Manufacturing Multi-Site “Cloud-based” Capstone Project, ASEE Annual Conf., 2012.

[19] Rouibah, K.; Ould-Ali, S.: Dynamic Data Sharing and Security in a Collaborative Product Definition Management System, Robotics and Computer-Integrated Manufacturing, 23(2), 2007, 217–233. http://dx.doi.org/10.1016/j.rcim.2006.02.011

[20] Shen, W.; Hao, Q.; Li, W.: Computer Supported Collaborative Design: Retrospective and Perspective, Computers in Industry, 59(9), 2008, 855–862. http://dx.doi.org/10.1016/j.compind.2008.07.001

[21] Winn, J.; Bright, T.; Jensen, C. G.; Teng, C.-C.: Using game server technology on fully distributed architectures for collaborative multi-user CAx applications, CoDesign: International Journal of CoCreate in Design and the Arts, 9(3), 2012, 178–189. http://dx.doi.org/10.1080/15710882.2013.824482

[22] Zender, F.; Schrage, D.; Richey, M.; Black, A.; Sullivan, J.; Gorrell, S.; Jensen, C. G.: Wing design as a symphony of geographically dispersed, multi-disciplinary, undergraduate students, 54th AIAA/ASME/ASCE/AHS/ASC Struct. Dyn. Mater. Conf., 2013.

[23] Zhang, D. Y.; Wang, L.; Zeng, Y.: Secure Collaborative Product Development : A Literature Review, International Conference on Product Life Cycle Management, 2008, 331–340.