Authority Management of Teamcenter Based on Rules

Xiaofeng Liu[a], Xiaoda Li[b, *], Xianghui Zhan[c] and Gangyu Wu[d]

Zhuhai College of Jilin University, Zhuhai 519041, China

[a]996364325@qq.com, [b]80831826@qq.com, [c]4186194@qq.com, [d]2997981905@qq.com

*Corresponding author

Keywords: PLM, Teamcenter, permission configuration, rules

Abstract: With the deepening of Industry 4.0, PLM technology has been recognized by more and more companies. This thesis mainly studies the permission configuration of PLM implementation Teamcenter and elaborates the method steps of permission configuration. This paper cuts through the principle of rights management, and describes the configuration scope, configuration rules and configuration scheme of key authority in detail, and implements the certification based on the above description to achieve the desired effect.

1. Introduction

Product Life Management (PLM) is an advanced product management solution. PLM system plays an important role in the enterprise, protects the intellectual property of the enterprise, ensures the uniqueness of product data, and carries out CAD/CAM/CAE. Integration enables collaborative design in the production process.

Teamcenter is a solution for PLM system. Teamcenter is mainly divided into five modules: project management module, process management module, organization management module and rights management module [1]. This paper mainly studies two permission setting modes of rights management in Teamcenter: object-based rights management and rule-based rights management.

2. Rule-based Authority Management Principle

Authority Management. Rights management refers to the licensing relationship when a person operates an object. Different objects and the same object in different states, people can operate different types of objects, these operations are controlled by permissions.
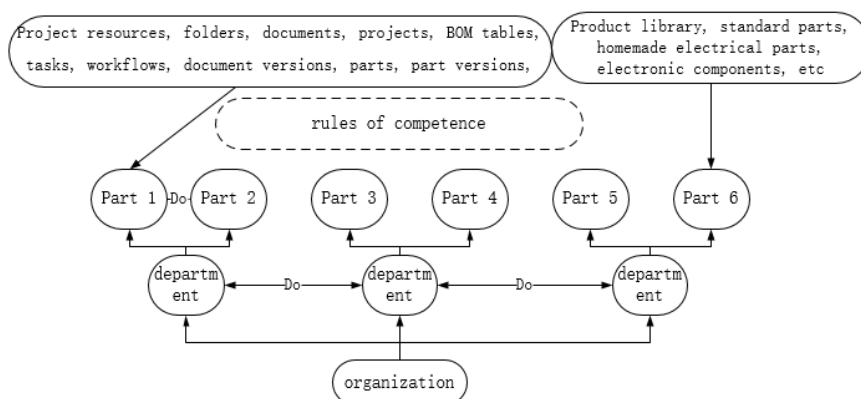

Figure 1. Rights Management Model

The authority management in TC is mainly based on the role management model, in which the subject, the operation authority and the object are the three elements of the authority management [2].

The organization personnel of the authority main body is mainly composed of three parts: group, role and user. Each user can have multiple roles, and each role can belong to different groups, which is consistent with the division of duties of the personnel in the real enterprise. The complexity of the organization's personnel determines the difficulty of privilege configuration in the product lifecycle system [3].

Rule Permission Definition. The rule-based permissions in the TC are mainly implemented in the form of a rule tree. As long as the rule permissions are defined according to certain rules, the rule permissions are stable in the TC, and the low modification frequency is the subject of the rights management in the TC. In addition, rule permissions can be called static permissions.

Limited Control Method for Data Security**.**

Control access to globally-based data.

Determine if the user has permission to view the object or perform an action on it.

Filter data based on the properties of the data.

They are granted access to data based on their user ID and their session environment (the groups and roles they use to log in).

Rules for Defining Rule Tree Permissions. The rules tree's permission rules are defined in three steps: conditions, the value of the condition, and the access control list (ACL) that grants access to the visitor.

The definition of permissions is complex and diverse. In order to make the set permissions clear, it is convenient for the system administrator to modify the permissions. The conditions of the permissions are divided into Has Bypass, Has Attribute, Has Class, etc.

3. Rule-based Permission Configuration

Configuration Elements. Access pattern of Teamcenter is mainly consists of four parts: the user metadata (group, role, user ID, permission level), the ACL access control lists (include reading, writing, copy, move out, etc.), object metadata (according to the type, owner, status, process, project such as partition), the rule tree (to decide when to apply an ACL to object).

According to Teamcenter's access pattern, permission configuration can be divided into two phases: rule tree setup, and ACL configuration.

Rule Tree Setup. The access manager is the main module for authority management in Teamcenter, and the authority rule tree has the underlying organizational structure in the access manager.

Basically all the underlying permissions are contained in the existing rule tree. The access controller can set two part permissions, con- trolled state data permissions (TCM release) and working permissions in design. New rule tree branches can be created in Teamcenter based on different phase attributes.

ACL Configuration. ACL configuration rule: The permission management configuration method in TC mainly consists of Access Control Entry (ACE) and Access Control List (ACL).

An access control list (ACL) is a collection of permissions owned by a series of visitor types. A visitor is a collection of users who share certain characteristics, such as people in the same project.

The matching relationship between each different visitor and its corresponding permissions is considered as an access control entry (ACE).One or more ACES constitute an ACL, in which different roles have different priorities in different groups. The stricter the restrictions are, the higher the priority will be.

Action type in ACE: User roles in Teamcener perform operations on objects such as read, write, delete, change permissions, copy, change ownership, publish, import, export, pass in, pass out, etc [4].
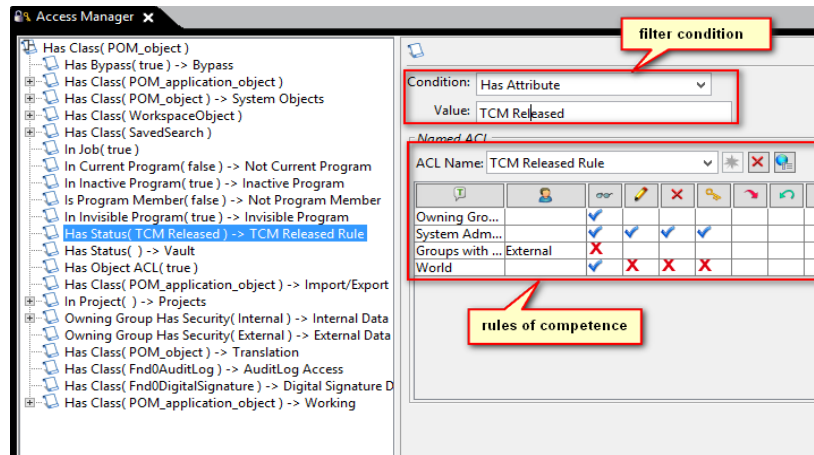
Access Configuration model:

Figure 2. Access Configuration

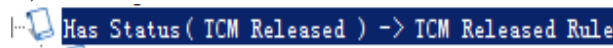Select the row on the left, as shown below:

Figure 3. Select the line

Operation area on the right:
Conditions: select conditions, such as [has attribute], that is, name as filter condition
Item Revision:
ItemRevision:object_desc=GFM
Data set:
Dataset:object_desc=GFM
Create a permission rule tree in the ACL, where you can type [SY_ACL_TEAM_GFM] if the product code is GFM

Enter ACL name: SY_ACL_TEAM_GFM and click the new button to generate permissions as shown below:
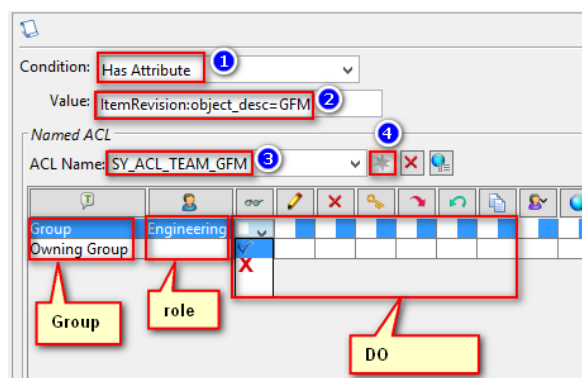

Figure 4. The configuration process

4. Implementation and Application of Rule-based Permission

Introduce the Company. Company A specializes in the design, development and operation of communication backup power supply, power backup power supply, UPS/EPS power supply, new energy storage power supply, power supply, photovoltaic system integration and other system solutions. It is an internationally renowned and domestically leading green energy manufacturer. Teamcenter will be adopted as the enterprise PLM solution in 2018.

Status Permission Configuration in Design. Files created by infodba are allowed to be accessed by users within information systems such as file templates Shared by administrators and historical

materials. This rule is placed on top of the other two denial of access rights, which have precedence over the following two rules.

Other common users create their own versions of objects and data sets only the creator and system administrator has access, others do not have access.
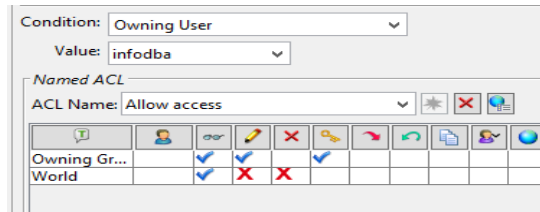

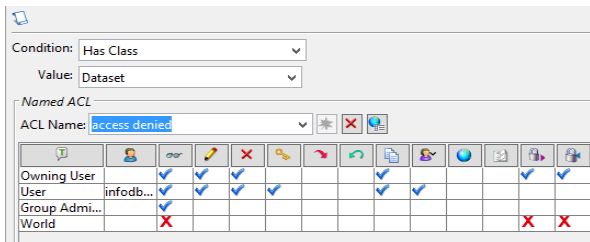Figure 5. Permissions on data created by the DBA
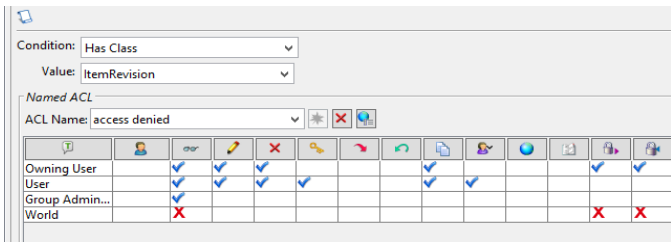

Figure 6. Dataset

Figure 7. ItemRevision

5. Summary

Teamcenter is a powerful system. At present, the software has been involved in various fields including military, aerospace, automotive, clothing, furniture, disposable products manufacturing. Project management and product life management, user rights management is an important part of it. User rights management regulates the operations that users can perform in the system, ensuring the security, integrity and sharing of data, and provides strong support for the establishment of workflow. Teamcenter has been well applied in practice.

Acknowledgements

References

[1] Yan Fei. Zhou, Ben. Ma, Linbo. Wang, etc.User Rights Management of Product Data Management System. Data Acquisition and Processing, 2002 (12), 385-389.

[2] Xing Chen, Research and Implementation of Workflow Technology in PLM [D], Mechanical Design and Theory, 57-63.

[3] Xiao li. Hong, Guo. Zhong. Zhang. Design and Implementation of Pdm Rights Management. Mechanical Manufacturing and Automation, 29-42.

[4] Xiao li. Hong, Guo Zhong. Zhang. (2007). Design and implementation of rights management based on teamcenter. Modern Manufacturing Engineering, 2007 (4), 25-28.