doi: 10.7690/bgzdh.2019.05.012

基于 Teamcenter 的弹箭产品权限控制

赵振杰[1]，王林林[1]，闫月晖[1]，张明星[1]，郭　欢[2]
（1. 北京航天长征飞行器研究所系统研发部，北京 100076；
2. 北京航天长征飞行器研究所技术保障处，北京 100076）

摘要：为解决航天弹箭产品在 3 维协同研制中对研制人员的权限、密级控制等要求较高的问题，提出一种基于 Teamcenter 系统权限解决方案。对权限控制基本要素、实现原理及过程进行阐述，通过二次开发技术实现了弹箭产品研制过程中权限控制管理的特定需求，并通过实际应用进行验证。应用结果表明：该方案增强了系统权限控制的易用性，有效地提高了弹箭产品在整个研制过程中的权限控制效率。

关键词：权限控制；规则树；访问控制列表；二次开发
中图分类号：TJ7　　**文献标志码：**A

Permissions Control of Missile and Rocket Products Based on Teamcenter

Zhao Zhenjie[1], Wang Linlin[1], Yan Yuehui[1], Zhang Mingxing[1], Guo Huan[2]
(1. *Research & Development Department of Hypersonic Vehicle*, *Beijing Institute of Space Long March Vehicle*, *Beijing* 100076, *China*; 2. *Department of Technology Support*, *Beijing Institute of Space Long March Vehicle*, *Beijing* 100076, *China*)

Abstract: In order to solve the problem of high demands of researchers' permissions and security classification in 3D collaborative development of the missile and rocket products, a solution to permissions control based on Teamcenter system is proposed. The basic elements, implementation principle and process are elaborated, by adopting secondary development technology, specific requirements of permissions control management in the process of missile and rocket products development are realized and practical application is verified. The results of application show that the scheme has enhanced the usability of system permissions control and efficiency of permissions control in the whole development process is effectively improved.

Keywords: permissions control; rule tree; access control list; secondary development

0　引言

弹箭产品的研制涉及总体、结构、控制、地面设备等多个专业，是一个需要不同专业人员共同参与的复杂协同工作过程。近年来，随着基于 MBD 的 3 维协同研制模式逐步推广，设计部门各专业以及设计与制造部门协同并行开展工作的模式已被普遍认可，在新型号研制中开展大量应用，研制效率和产品质量均得到提升。Teamcenter 作为一种产品全生命周期管理系统，提供了项目管理、权限管理、产品结构管理等产品全生命周期管理解决方案，有效地把人、过程、信息集成在一起，支持与产品相关的协同设计、权限管理、信息分发与反馈等多环节的控制[1-4]。

弹箭产品除了具备控制严格、分配灵活、运行高效等一般特点外，还需满足动态变化、密级管理、易用性强的涉密产品管理需求。笔者在 Teamcenter 系统固有模块基础上，通过二次开发技术对已有权限控制功能进行扩展，达到弹箭产品设计数据按项目、角色、密级等分类控制产品权限的目标，实现集成产品开发团队的每一个成员因专业、密级不同分配详细的控制权限，保证全生命研制周期内产品数据在正确的条件下被授权的人员访问。

1　权限概述

1.1　权限控制要素

Teamcenter 作为产品研制过程的全生命周期管理系统，对设计、制造过程中产生的设计、工艺、流程等各类数据进行统一、集中式管理，以便于数据长期存储和数据共享。Teamcenter 系统通过用户安全访问管理机制来实现，可以防止系统中存储的产品数据被非法访问或误操作。所谓权限是指 Teamcenter 系统中某个或某类访问者对于处于某个特定环境下，某类数据对象类型是否具有执行某个动作的权利。如图 1 所示， Teamcenter 的权限控制要素通常由访问者、数据对象和操作组成[5]。

收稿日期：2019-02-18；**修回日期：**2019-03-01
作者简介：赵振杰(1981—)，男，北京人，硕士，从事产品数据管理、数字化设计与制造研究。

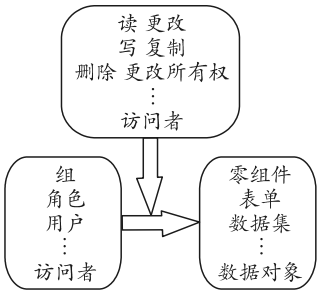

图 1　权限控制三要素

1.2　用户操作权限

Teamcenter 中用户操作权限主要包括读、写、删除、复制、检出/检入、导入/导出、指派项目等，对用户分配权限时依据最小化的原则，即在满足用户操作需求的条件下权限越小越好，以防用户对系统内其他数据进行非法访问。

操作权限分配时应考虑密级要求，即高密级用户按要求可以访问低密级或同密级数据，但低密级用户不能访问高密级数据。

1.3　权限控制方式

Teamcenter 中有 2 种访问控制方式：一种是基于规则的权限控制方式，是指通过设置权限规则，将系统中某类特定的对象授权给具有共性的访问者访问，同一类对象可以设置多条权限规则，最终形成一个权限规则树，在规则树中采用“顶端优先于底端，子级优先于父级”的优先级别；另一种是基于对象的权限控制，是指将某个具体的对象授权给某用户、组、角色访问。

2　二次开发关键技术

Teamcenter 二次开发分为客户端和服务端开发。Teamcenter 提供 4 种与外部程序进行交互的接口方式，即 RC、ITK、SOA、Generic Shell，其中 RC 和 ITK 是最为常用的接口开发方式[6]。客户端开发采用 Java 语言和 Eclipse 工具进行开发，服务端的开发采用 C 语言及集成工具包(intergrated toolKit，ITK)实现。

2.1　客户端开发

客户端开发主要用于在 Teamcenter 系统中扩展菜单、视图、透视图等，依据用户需求开发特定功能的对话框、操作界面等。本方案中，客户端开发主要涉及创建、派生及扩展产品工作区菜单功能。

2.2　服务端开发

服务端的开发由应用层和核心层构成。应用层由对象接口组件适配器(object I/F comp adapters)、应用对象(application objects)和应用(Applications)组成；核心层由 POM(persistent object manager)管理器和数据库 I/O 模块(database I/O module)组成[7]。

服务器端的全部功能模块是建立在一组集成开发工具(ITK)之上的应用模块，用户可以利用 ITK 扩展 Teamcenter 系统功能，与第三方软件或用户自主开发软件的集成。ITK 开发包括内部和外部 ITK 程序 2 种。内部 ITK 程序必须在客户端注册后由系统接口调用，如 Handler 程序，*.dll 程序等；外部 ITK 程序为单独运行的可执行程序，如*.exe 等，在服务端由批处理程序直接调用。在本方案中，服务端的开发主要涉及项目自动指派和流程 Handler 的开发。

3　权限控制实现

权限控制主要基于 Teamcenter 系统的建立集成产品开发团队、配置权限规则和系统二次开发，以实现弹箭产品研制过程中的权限控制管理。

3.1　建立集成产品开发团队

在项目研制初期，项目管理员在系统中建立一个新的项目，并指派项目小组管理员，可以修改项目信息、添加/移除小组成员、为项目小组成员设置特权。

3.1.1　初始化产品工作区

项目小组管理员在系统中创建本项目的专属工作区，用于统一组织和存放产品设计相关技术资料。产品工作区的创建或扩展由客户端二次开发功能实现。如图 2 所示，项目小组管理员既可以手工创建产品工作区，又可以依据系统定义的产品工作区为模板派生产品工作区。如图 3 所示，在建立产品工作区后，项目小组管理员可对产品工作区进行扩展或删除，完成产品工作区的初始化工作。

图 2　二次开发菜单

图 3　初始化产品工作区

3.1.2　指派项目小组成员

项目小组管理员在产品工作区创建完毕后，依据型号产品设计任务分工需求，从系统组织结构中

为项目添加成员，项目小组成员对整个项目的产品数据只具有浏览的权限，如果需要为项目指派或移除设计数据，则由项目小组管理员为其分配特权。指派后的项目小组成员如图 4 所示。

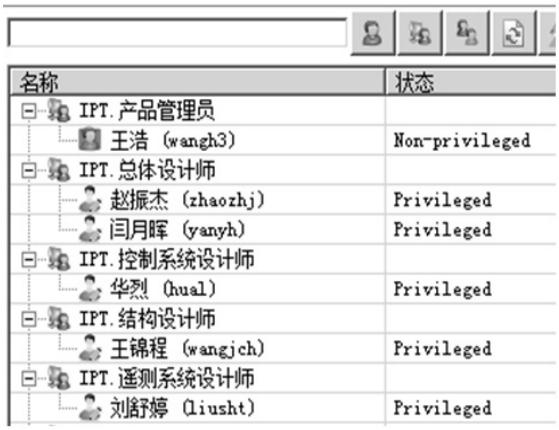

图 4 指派项目小组成员

3.2 权限规则定义

3.2.1 权限设计原则

项目小组内的所有成员对本项目所属的产品数据具有查询、浏览的权限；项目小组内的特权成员具有向本项目指派数据或从本项目中移除数据的权限；项目小组外的成员默认不具有查询、浏览本项目内所有数据的权限。

工作状态中的产品数据，其所有者可对数据进行浏览、更改、删除等操作；流程状态中的产品数据，其所有者对数据具有查询、浏览、批注权限；已发布状态的产品数据，其所有者只对数据具有查询、浏览权限。

在密级控制方面：严禁用户创建高于用户密级的产品设计数据；严禁低密级人员查询或浏览高密级产品设计数据。

3.2.2 访问规则的定义

在 Teamcenter 系统中，使用访问规则将权限控制与数据对象进行关联，访问规则由条件、值和对应的访问控制列表(access control list，ACL)组成[8]，即对满足某种条件的数据对象具有 ACL 中定义的操作权限。

1) 项目中权限规则。

项目组的成员基于项目角色来实现访问控制，项目管理员通过为项目创建合适的 ACL，以创建或修改用户对项目产品设计数据的访问规则，结合弹箭产品设计数据对用户密级要求较严，项目中定义的 ACL 如表 1 所示。

表 1 项目中 ACL 定义

权限	Owning User	User Under IP Clearance	Project Teams	World
读	√	×	√	×
写	√		×	×
删除	√		×	×
更改	√		×	×
复制	√		×	×
签入/签出	√		×	×
批注	√		×	×
提升	√		×	×
退回	√		×	×

2) 数据状态的权限规则。

产品数据状态主要分为工作中、流程中和已发布 3 个状态。流程中权限规则定义见下文，工作中和已发布状态的 ACL 定义如表 2、表 3 所示。

表 2 工作中状态的 ACL 定义

权限	Owning User	User Under IP Clearance	World
读	√	×	√
写	√		×
删除	√	×	×
更改	√		×
复制	√		×
签入/签出	√		×
批注			×
提升	√	×	×
退回	√		×

表 3 已发布状态的 ACL 定义

权限	Owning User	World
读	√	√
写	×	×
删除	×	×
更改	×	×
复制	√	×
签入/签出	×	×
批注	×	×
提升	×	×
退回	×	×

3.3 项目自动指派

Teamcenter 中的项目应用程序提供了对数据组织、访问控制和管理的功能，项目组中具有特权的成员可以向项目指派数据，只有指派后的产品设计数据才具有本项目设置的相关权限。由于 Teamcenter 系统只具备手工向项目中指派数据的功能，易用性较差。笔者通过对服务端进行二次开发，当设计员在项目的工作区新建产品设计数据或将已创建的产品设计数据拖拽到项目工作区时，由二次开发程序自动将对产品设计数据进行项目指派，提高了基于项目进行产品数据权限控制的应用效率。二次开发关键程序代码如下：

```
WSOM_ask_object_type2(targetFolderTag,&obj
```

```
Type);
    printf("the target folder type is %s\n",objType);
    if(tc_strcmp(objType,"CZ6Folder")!=0){
     printf("the target folder type is not CZ6Folder ignore!!\n");
     goto CLEANUP;
    }
    AOM_ask_value_tags(targetFolderTag,"project_list",&folderPCount,&folderProjects);
    if(folderPCount<1){
     printf("target folder don't have any projects ,exit!\n");
     goto CLEANUP;
    }
    POM_AM__set_application_bypass(true);
    for(i=0;i<count;i++){
     tag_t tempTag = setObjs[i];
     GTCTYPE_is_type_of(tempTag,"Item",&isItem);
     GTCTYPE_is_type_of(tempTag,"ItemRevision",&isRev);
     if(!isItem&&!isRev){
      continue;
     }
     ifail = PROJ_assign_objects(folderPCount,
     folderProjects,1,&tempTag);
     if(ifail==ITK_ok){
      printf("指派项目成功！");
     }}
    ……
```

3.4　动态权限控制

动态权限控制主要是指流程中的权限控制，即发起工作流程后，根据流程步骤的不同需要为该步骤的执行者动态授予相应操作的权限，当该流程步骤结束时，权限被自动收回[9-11]。动态权限设置包括流程 ACL 定义及 Handler 程序开发。

3.4.1　流程 ACL 定义

在数据审签流程中，需要在不同的流程审签节点中为相应的审签人员分配权限。以产品设计审签流程为例，在流程中的设计节点，数据对象所有者需要对数据进行修改操作，因此需要分配读、写、检入/检出等权限。设计节点 ACL 定义如表 4 所示。在流程的其他节点，如工艺会签、标审等，审签人员只需对数据进行查看、批注等简单操作。其他节点 ACL 定义如表 5 所示。

表 4　设计节点 ACL 定义

权限	Approver	Owning User
读	√	√
写	×	√
删除	×	√
更改	×	√
复制	×	√
签入/签出	×	√
批注	×	√
提升	×	√
退回	×	√

表 5　审签流程其他节点 ACL 定义

权限	Approver	Owning User
读	√	√
写	×	×
删除	×	×
更改	×	×
复制	×	√
签入/签出	×	×
批注	√	√
提升	×	√
退回	×	√

3.4.2　Handler 程序开发

在发起工作流程时，系统通过二次开发 Handler 程序，对流程发起者是否是数据的所有者以及流程各节点审核用户的密级是否低于数据密级的情况进行核验，以控制产品数据流程发起权限及高密级数据指派低密级用户审核的违规现象发生。校验流程发起者是否是数据所有者的 Handler 关键程序如下：

```
EPM_ask_job( msg.task, &job );
EPM_ask_root_task( job, &root_task );
//获取所有 attachment 对象
EPM_ask_attachments(root_task,EPM_target_attachment,&attach_object_count,&attach_object_tags);
 if (attach_object_count==0)
 { decision = EPM_go;  }
 else{
 CALL_IN_RULE(SA_ask_current_groupmember(&CurGroupMember));
 CALL_IN_RULE(AOM_get_value_tag(CurGroupMember,"user",&CurUser));
 CALL_IN_RULE(AOM_get_value_string(CurUser,"user_id",&curuserStr));
 for(i=0;i<attach_object_count;i++){
  CALL_IN_RULE(AOM_ask_owner(attach_object_tags[i],&tag_owner));
  CALL_IN_RULE(AOM_ask_value_string(tag_owner,"user_id",&owner_name));
  if(0!=tc_strcmp(owner_name,curuserStr)){E-
```

```
MH_sEMH_store_error(EMH_severity_user_error,WORKFLOW_ERROR1);
        ifail=WORKFLOW_ERROR1;
        EMH_ask_error_text(ifail, &message);
        printf("error is [%s]", message);
        decision = EPM_nogo;
        break;
    }   }   }
```

程序运行效果如图 5 所示。

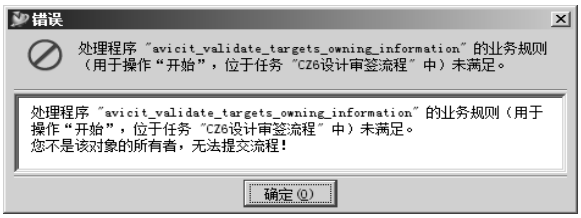

图 5 校验流程发起者

检验流程各节点审核用户的密级是否低于数据密级的 Handler 关键程序如下：

```
// 获取流程目标中的对象密级列表
CALL_IN_RULE(PREF_ask_char_values("IP_level_list_ordering",&classification_count,&preValue));
    for(i=0;i<attach_object_count;i++)
    {
    CALL_IN_RULE(AOM_ask_value_string(attach_object_tags[i],"ip_classification",&tmpIpStr));
    for(m=0;m<classification_count;m++){
    if(strcmp(preValue[m],tmpIpStr) == 0){
       if (hign_index < m){
        hign_index = m;
        break;
    } }   }   }
          ……
//获取流程中人员密级列表 CALL_IN_RULE(AOM_get_value_string(respUser,"user_name",&doUserStr));
    CALL_IN_RULE(AOM_get_value_string(respUser,"ip_clearance",&tmpIpStr));
    for(m=0;m<classification_count;m++){
    if(strcmp(preValue[m],tmpIpStr) == 0){
     ip_flag = true;
     obj_index = m;
     break;
    }}
    if (obj_index < hign_index){
       valid_flag = true;
       decision = EPM_nogo;
    }
```

程序运行效果如图 6 所示。

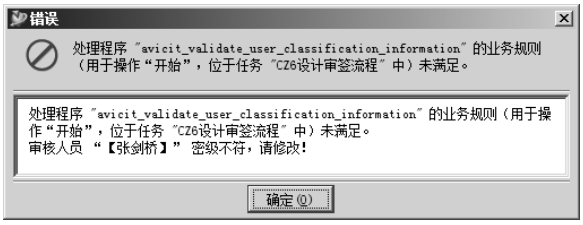

图 6 校验审核用户密级

4 结束语

笔者通过对 Teamcenter 系统权限控制要素进行分析，结合系统二次开发技术对权限控制功能进行扩展，满足了弹箭产品 3 维协同研制过程中人员权限控制、密级管理等相关需求。在某飞行器型号产品研制过程中进行应用验证，结果证明该方案合理、可行，可为实现弹箭产品协同研制全生命周期管理过程中数据权限控制提供解决方案。

参考文献：

[1] SUN Y, HAN L, LI N, et al. Research and application of PLM in SBA[J]. Journal of System Simulation, 2008, 20(19): 5166-5167.

[2] VEZZETTI E, VIOLANTE M G, MARCOLIN F. A Benchmarking Framework for Product Lifecycle Management(PLM) Maturity Models[J]. The International Journal of Advanced Manufacturing Technology, 2014, 71(5-8): 899-918.

[3] 王磊. 基于 PLM 的挖掘机协同设计研究[D]. 天津: 天津大学, 2014: 5-6.

[4] 廖文和, 杨海成. 产品数据管理技术[M]. 南京: 江苏科学技术出版社, 2006: 56-61.

[5] 黄曙荣, 安晶, 王伟, 等. 产品数据管理 PDM 原理与应用[M]. 镇江: 江苏大学出版社, 2014: 95-96.

[6] 陈冠华. PDM 系统实施与二次开发技术应用研究[D]. 长沙: 中南大学, 2011: 40-41.

[7] 朱文华, 王大斌, 苏玉鹏. Teamcenter Engineering 中 BOM 功能的二次开发[J]. 现代制造工程, 2009(2): 40-44.

[8] 安晶, 殷磊, 黄曙荣. 产品数据管理原理与应用[M]. 北京: 电子工业出版社, 2015: 212-213.

[9] ROSHAN T, RAVI S. Task-based Authorization Controls(TBAC): A family of models for active and enterprise-oriented authorization management, Database Security XI[J]. Status and Prospects, Chapman & Hall, 1998(8): 121-128.

[10] 李姝宁, 陈恳, 杨东超. 基于 PDM 的权限管理研究[J]. 机械设计与制造, 2005(1): 122-124.

[11] 于戈, 宋宝燕, 田文虎. 现代集成制造中的工作流管理技术研究[J]. 计算机集成制造系统-CIMS, 1999, 5(6): 8-11.