铁路计算机应用
RAILWAY COMPUTER APPLICATION

铁路建设行业内容管理权限模型的设计与实现

吕向茹，牛宏睿，卢文龙

Authority model of content management for railway construction industry

LYU Xiangru, NIU Hongrui, and LU Wenlong

引用本文:
吕向茹, 牛宏睿, 卢文龙. 铁路建设行业内容管理权限模型的设计与实现[J]. 铁路计算机应用, 2022, 31(6): 24–29.
LYU Xiangru, NIU Hongrui, LU Wenlong. Authority model of content management for railway construction industry[J]. Railway Computer Application, 2022, 31(6): 24-29.

在线阅读 View online: http://tljsjyy.xml-journal.net/2022/I6/24

文章编号：1005-8451（2022）06-0024-06

铁路建设行业内容管理权限模型的设计与实现

吕向茹[1]，牛宏睿[2]，卢文龙[2]
（1. 北京经纬信息技术有限公司，北京 100081；
2. 中国铁道科学研究院集团有限公司 电子计算技术研究所，北京 100081）

摘 要：铁路建设行业存在巨大的内容管理需求，针对非结构化数据治理难、内容管理要求高、多层级权限管控复杂等问题，结合铁路建设内容管理权限控制特点，在基于角色的访问控制模型基础上设计并实现了铁路建设行业内容管理权限模型。将其应用于铁路建设内容管理系统，通过基础权限和角色授权的配置，该模型满足了多层级、精细化内容管理需求，实现了项目信息共享与交互。

关键词：铁路建设；内容管理；访问控制；授权机制；权限模型
中图分类号：U2 : TP39 **文献标识码：**A **DOI：**10.3969/j.issn.1005-8451.2022.06.05

Authority model of content management for railway construction industry

LYU Xiangru[1], NIU Hongrui[2], LU Wenlong[2]
(1. Beijing Jingwei Information Technologies Co. Ltd., Beijing 100081, China;
2. Institute of Computing Technologies, China Academy of Railway Sciences Corporation Limited, Beijing 100081, China)

Abstract: There is a huge demand for content management in the railway construction industry. In view of the difficulties in unstructured data governance, high requirements for content management and complex multi-level authority control, combined with the characteristics of railway construction content management authority control, this paper designed and implemented the authority model of the content management for railway construction industry based on the role-based access control model. The model was applied to the railway construction content management system. Through the configuration of basic authority and role authorization, the model meets the requirements of multi-level and refined content management, and implements the sharing and interaction of project information.

Keywords: railway construction industry; content management; access control; authorization mechanism; authority model

数据是铁路实现数字化转型的关键，是铁路百年工程的源头，也是打造智能化铁路的基石[1]。其中，非结构化数据是数据治理的难点，约占铁路建设行业总数据量的 80%。铁路建设行业内容管理是对铁路建设期间形成的各类非结构化数据的管理，主要包括文本、图片、设计模型、设计图纸、各类报表、公文、视频、音频等[2]。铁路建设内容管理不仅要满足建造期数据高效运转，还需为铁路运营和维护完成原始数据积累。通过内容管理可深度挖掘铁路建设行业数据价值，提高行业竞争优势，为行业长远发展提供助力。

收稿日期：2022-03-01
基金项目：中国国家铁路集团有限公司科技研究开发计划重点课题（N2020S011）
作者简介：吕向茹，工程师；牛宏睿，高级工程师。

权限控制是实现内容多层级精细化、高效化管理的重要手段，同时也为铁路行业内容管理提供安全保障[3]。为满足铁路建设单位和参建单位精细化内容访问控制，保障铁路建设内容管理安全可靠，亟需设计一套适用于铁路建设行业内容管理的权限模型[4]。

1 权限模型分类及权限控制特点

1.1 权限模型分类

权限控制即控制用户对资源或服务的访问权限，目前常见的权限模型包括访问控制列表（ACL，Access Control List）模型、基于属性的访问控制（ABAC，Attribute-Based Access Control）模型、基于角色的访问控制（RBAC，Role-Based Access

Control）模型等，不同权限模型适用于不同的应用场景。

（1）ACL 权限模型

ACL 是一种以资源为核心，基于权限列表进行授权的访问控制机制。模型主要包含用户、资源和操作 3 个关键要素。当用户请求操作资源时需检查资源的权限列表，如果资源的权限列表中存在该用户的操作权限则允许，否则拒绝。ACL 权限模型的优点在于原理简单，缺点在于当存在大量用户或资源众多的情况下，不能满足基于复杂多层级目录树内容管理的需求。

（2）ABAC 权限模型

ABAC 通过实体、操作、环境等属性集合来实现用户对资源的访问控制，是一种基于属性的访问控制模型，如图 1 所示。ABAC 将用户按照不同属性进行划分，为具有各类属性组合的用户进行资源授权。ABAC 权限模型的优点是能够满足复杂场景下权限的灵活配置，缺点是授权机制较为复杂。而铁路建设行业内容管理的授权过程面向普通用户，因此需要满足简单、易操作等特性。

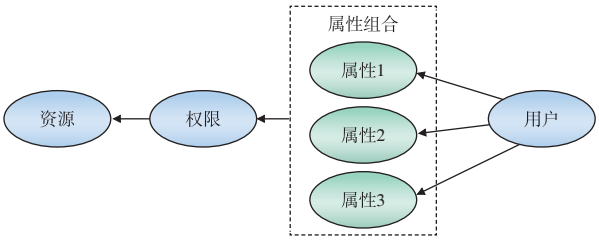

图1　ABAC 权限模型

（3）RBAC 权限模型

RBAC 指基于角色的访问控制，是目前最常用的一种权限模型[5]。RBAC 模型包括用户、角色、操作、对象和权限 5 个基本要素。在 RBAC 模型分类中，RBAC0 定义了最小要素几何，也是其他 RBAC 模型的基础，其权限模型如图 2 所示。该模型在对象和操作之间构建对应关系，形成权限项并授权于角色，通过会话实现用户和角色的映射关系[6]。RBAC 权限模型的继承机制和职责分离机制为铁路建设行业内容管理权限控制模型提供了借鉴和参考。

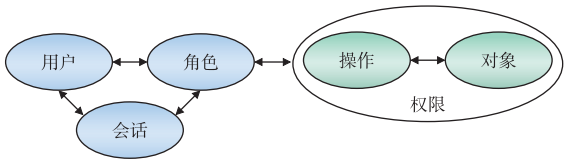

图2　RBAC0 权限模型

1.2　权限控制特点

铁路建设行业发布了《铁路建设项目资料管理规程》《竣工文档管理办法》等一系列文件用以规范铁路建设项目立项、审批、招投标、勘察设计、施工、监理、竣工验收等全生命周期内文档的形成、收集、整理、组卷、验收、归档和移交等管理。通过规范化管理，铁路建设行业内容管理权限控制形成以下特点。

（1）授权对象为文件夹或文件节点

在一般权限模型中，授权对象是指模型化的应用程序编程接口对象，包括 Pods、Nodes、Secrets、ConfigMaps、Deployments 等，而基于内容管理的授权对象指文件夹和文件形成的节点。

（2）授权对象具有多层级继承关系

在一般权限模型中，授权对象多是对单层级资源进行的分类；而基于内容管理的文件夹和其子文件夹或文件本身具有继承关系，因此需要针对具有继承关系的多层级目录树节点对象进行授权。

（3）具有统一的标准化目录结构

依据《铁路建设资料管理规程》，将铁路建设内容管理标准目录结构划分为 5 类，包括 A 类—建设管理资料、B 类—勘察设计资料、C 类—施工资料、D 类—监理资料、E 类—竣工验收资料[7]。

（4）元数据以 JSON Schema 的方式挂接在节点

铁路建设行业已梳理 4 191 条元数据，这些元数据以结构化数据方式进行存储，以 JSON Schema 的方式挂接在节点，通过构建元数据模型实现对元数据的组织和管理，对节点进行授权的同时即可实现对元数据的操作授权。

（5）实行分级授权的管理模式

铁路建设行业内容管理通过先创建节点、后进行授权的方式对铁路建设结构化数据和非结构化数

据进行管理。系统管理员创建“项目”节点，并将“项目”节点管理权限授权给项目管理员，项目管理员再依据需求创建“单位资料库”，并将“单位资料库”节点管理权限授权给单位管理员，单位管理员再依次创建本单位项目目录结构并进行授权。

2 权限模型设计与实现

2.1 权限模型

铁路建设行业内容管理权限模型在 RBAC 权限模型基础上，以节点为核心进行授权，每个节点都存在一个权限列表与其对应，权限列表包含一条或多条权限控制项，权限控制项包括权限所有者和对应的角色，角色中包含了多个基础权限，其模型如图 3 所示[8]。

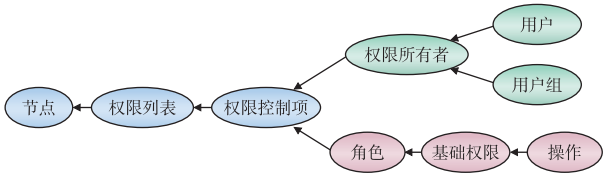

图3 铁路建设行业内容管理权限模型

（1）节点：铁路建设内容管理授权对象，包括文件夹和文件 2 类，不同于一般权限模型中的资源或对象，内容管理对象具有继承关系。

（2）权限列表：授权对象的访问控制列表，由一条或多条权限控制项组成。

（3）角色：一系列基础权限的组合，铁路建设行业内容管理权限模型中的角色设定具有继承关系。

（4）基础权限：针对节点和子节点进行设定，包括读、写、删除、属性查看、属性编辑等。

（5）操作：包括查看、下载、删除、重命名、修改等，用户具有的操作权限由基础权限决定。

2.2 权限映射

铁路建设行业内容管理权限模型的设计需满足在不修改权限体系的情况下，通过简单配置即可实现权限扩展，满足未来更高精细化管理需求。本文提出的权限模型通过固化基础数据权限，依托基础权限组合授权的方式简化授权操作来实现，同时通过基础数据权限对操作权限的约束，避免操作权限的频繁变更对权限体系带来的影响。基础权限、角色和操作的映射关系如图 4 所示。

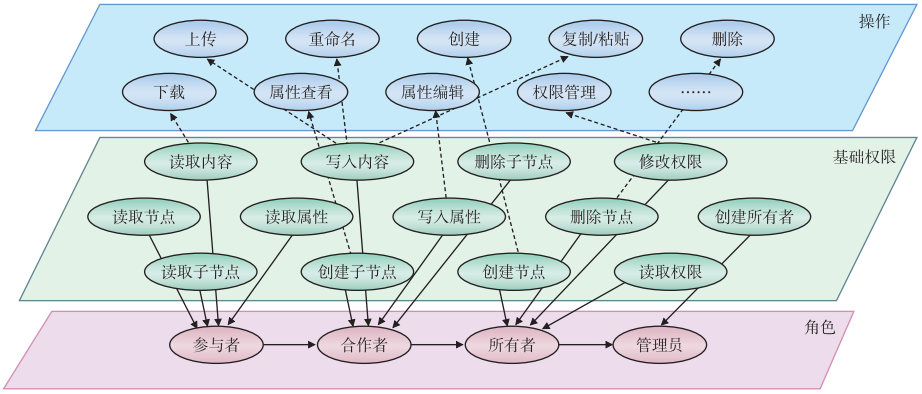

图4 基础权限、角色和操作的映射关系

（1）基础权限

铁路项目内容管理权限模型定义了 13 项固化基础权限，如表 1 所示。

（2）角色

铁路项目内容管理权限模型定义了 4 类角色，如图 5 所示。用户可根据自身需求进行扩展和配置。参与者为最小权限集合；在参与者基础上增加写入内容、写入属性、创建子节点和删除子节点形成合作者角色；在合作者角色的基础上增加创建节点、删除节点、读取权限和修改权限形成所有者角色；为所有者角色增加创建所有者基础权限后形成管理者角色。

（3）操作

操作权限包括上传、下载、重命名、属性查看、

表1　基础权限类型列表

序号	基础权限类型	作用于文件夹	作用于文件
1	读取节点	限制读取该文件夹的名称	限制读取该文件名称
2	读取子节点	限制读取子文件夹/文件的名称	/
3	读取内容	/	限制读取文件内容
4	读取属性	限制读取该文件夹属性	限制读取该文件属性
5	创建节点	限制该文件夹名称的修改	限制该文件名称的修改
6	创建子节点	限制创建子文件夹/文件	/
7	写入内容	/	修改文件内容
8	写入属性	限制新建、修改、删除该文件夹的属性	限制新建、修改、删除该文件的属性
9	删除节点	删除该文件夹及所有子节点	删除该文件
10	删除子节点	限制删除该文件夹的子节点	/
11	读取权限	限制读取该文件夹的权限许可	限制读取该文件的权限许可
12	修改权限	限制写入和修改该文件夹的权限	限制写入和修改该文件的权限
13	创建所有者	限制设定文件夹所有者	限制设定文件所有者

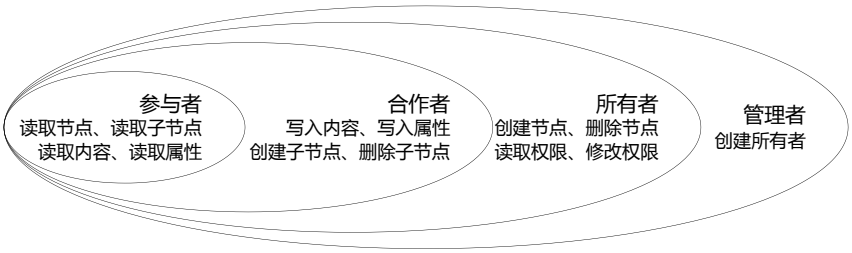

图5　角色类型和角色关系

创建、复制/粘贴、删除、属性编辑等，操作权限受基础权限的约束，例如用户是否具有下载权限，取决于用户所被授予角色中是否包含读取内容权限。

2.3　授权机制

通过创建灵活、简单的授权机制，实现铁路建设单位和参建单位分级授权，满足铁路建设内容管理需求。铁路建设行业内容管理授权机制主要包括权限设定、权限查看、权限继承、权限删除和权限判断等。

（1）权限设定

创建节点后判断是否需要修改节点权限，若不需要修改，则自动继承父节点权限；若需要修改，则需对权限列表进行扩展，新增 2 条权限列表数据，一条为自定义权限，另一条为共享权限。添加权限列表数据后再判断是否需要新增权限控制项，若需要新增权限控制项，则需在权限列表和权限控制项关系表中增加权限列表和权限控制项关联关系。

（2）权限查看

通过获取节点 ID 查找节点表中节点关联的权限列表 ID，进而查询权限列表和权限控制项关系表中权限列表 ID 对应的权限控制项，返回对应的权限控制项。

（3）权限继承

创建子节点时默认继承父节点权限，子节点自动获取父节点权限列表 ID 对应权限控制项。若取消子节点继承关系，则权限列表中的继承字段设为假，并新增权限列表数据项。

（4）权限删除

删除节点权限时需先删除权限列表和权限控制项关系表中的权限列表和权限控制项，此外还需删除继承此节点权限的权限控制项，继承的权限项通过权限列表和权限控制项关系表中的位置字段来判断，位置序号大于此节点的权限项需删除。

（5）权限判断

首先获取用户节点列表，通过节点列表获取节点对应的权限列表 ID，进而获取权限列表 ID 对应权限控制项，查找基础权限对应的操作权限，返回用

户操作列表。

2.4 授权流程

依据铁路项目内容管理需求，系统管理员创建铁路项目资料库，为项目管理员授权管理者角色；项目管理员创建建设单位资料库、设计单位资料库、施工单位资料和监理单位资料库，并将各单位管理员授权管理者角色；各单位管理员登录系统，根据各单位内容管理需求创建各单位资料库，其中建设单位管理员分别为工程部和质安部文件夹授权。部分资料库目录树如图 6 所示。通过分级授权项目管理员、单位管理员和文档所有者可实现设定、查看、判断和继承权限。

当施工单位管理员对本单位“线路综合”文件夹重新进行授权时，取消线路综合文件夹的继承权限，图 6 中的“线路”与“线路综合”文件夹的继承链断开。重新对“线路综合”文件夹进行自定义授权时，同时生成 2 条权限数据,分别为自定义权限和共享权限,“线路综合”文件夹对应的节点权限为自定义权限,“水准表”文件继承“线路综合”文件夹节点的权限，水准表文件对应的节点权限为共享权限。铁路建设单位和各参建单位基于本文设计的权限控制模型可灵活配置和修改各单位职责范围内的内容访问权限。

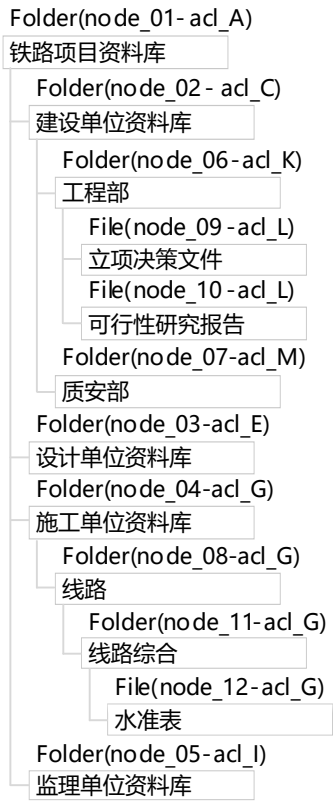

图6 资料库目录树

3 权限模型应用

依据本文设计并实现的铁路建设行业内容管理权限模型，搭建了铁路建设内容管理系统，对铁路建设项目立项、审批、招投标、勘察设计、施工、监理、竣工验收等全生命周期内文档进行统一管理。铁路建设内容管理系统以电子文档全过程管理为指导思想，针对权限精细化管控需求进行模块化设计，具有高内聚、低耦合的特点。

铁路建设内容管理系统权限管理模块如图 7 所示，通过基础权限、角色授权配置，满足了铁路建设多层级、细粒度内容管理需求，实现了铁路建设项目信息共享与交互；通过统一的文档创建、存储、流转、利用和归档，推动了铁路建设项目的信息化、标准化管理。

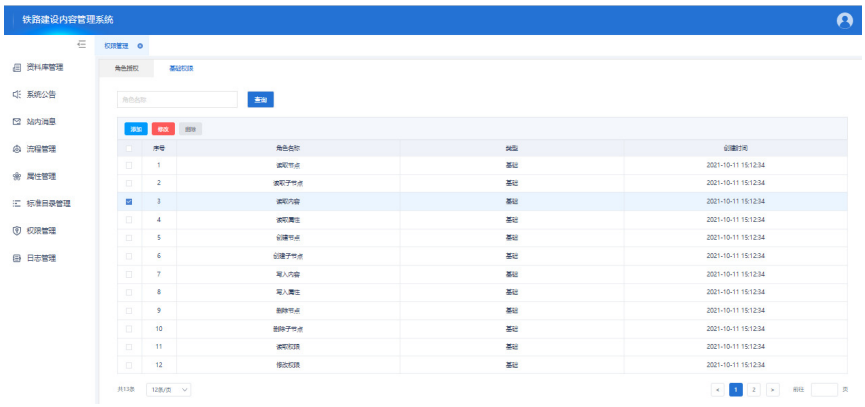

图7 铁路建设内容管理系统权限管理

4 结束语

铁路建设行业存在巨大的内容管理需求。本文设计了一套适用于铁路建设行业内容管理的权限模型；对权限模型、权限映射及权限设定、查看、继承、删除、判断等授权机制和授权流程进行研究，并通过搭建铁路建设内容管理系统予以应用，满足了铁路建设单位和参建单位灵活化、个性化、高效化管理需求，同时也为铁路建设行业内容管理提供了通用解决方案。该模型对于提高企业竞争力，助力铁路数字化转型，进而打造智能铁路具有积极意义。

参考文献

[1] 王同军. 中国智能高铁发展战略研究 [J]. 中国铁路，2019（1）：9-14.

[2] 程志华，倪时龙，黄文思，等. 企业级非结构化数据管理平台研究及实践 [J]. 电力信息化，2012，10（3）：12-20.

[3] 王同军. 智能铁路总体架构与发展展望 [J]. 铁路计算机应用，2018，27（7）：1-8.

[4] 朱 庆，李函侃，曾浩炜，等. 面向数字孪生川藏铁路的实体要素分类与编码研究 [J]. 武汉大学学报（信息科学版），2020，45（9）：1319-1327.

[5] 陈占芳，顾 健，张晓明，等. 一种超细粒度权限模型研究与应用 [J]. 长春理工大学学报（自然科学版），2016（1）：88-90.

[6] 白嘉萌，寇英帅，刘泽艺，等. 云计算平台基于角色的权限管理系统设计与实现 [J]. 信息网络安全，2020（1）：75-82.

[7] 铁道部经济规划研究院. 铁路建设项目资料管理规程：TB10443[S]. 北京：铁道部经济规划研究院，2010.

[8] Caruana D. Professional Alfresco: Practical Solutions for Enterprise Content Management [J]. Wiley & Sons, 2010, 150(2): 210-215.

责任编辑 朱 一