文章编号：1005-8451（2016）04-0045-04

RBAC模型在西安干部履责管理系统中的应用

关则彬[1]，蒋　荟[1]，唐丹玉[2]，陶　承[1]，陈　雄[1]
（1.中国铁道科学研究院　电子计算技术研究所，北京　100081；
2. 北京航天世景信息技术有限公司，北京　100089）

摘　要：西安干部履责管理信息系统的用户数量庞大，用户权限管理错综复杂。本文对西安干部履责系统中引入基于角色访问控制（RBAC）模型来解决用户的权限管理问题进行了一定的改进。介绍西安干部履责系统用户权限管理的业务需求以及RBAC模型的基本思想。论述该系统中用户权限管理的功能设计、实现技术框架和数据库设计等。实践表明，利用RBAC模型来解决西安干部履责系统用户权限管理可取得良好的实际应用效果。

关键词：RBAC模型；权限管理；干部履责管理系统
中图分类号：U29：F530.64：TP39　**文献标识码：**A

RBAC Model applied to Xi'an Cadres Fulfillment Responsibilities Management System

GUAN Zebin[1], JIANG Hui[1], TANG Danyu[2], TAO Cheng[1], CHEN Xiong[1]
(1. Institute of Computing Technologies, China Academy of Railway Sciences, Beijing　100081, China;
2. Beijing Aerospace Scene Information Technology Co. Ltd., Beijing　100089, China)

Abstract: There are huge numbers of users for the Xi'an Cadres Fulfillment Responsibilities Management System (FCRMS). User rights management is very complicated. In this article, it was introduced the role based access control (RBAC) model to solve the problem of user authority management in FCRMS. The article described business needs of the user rights management and the basic idea of RBAC model, discussed the function design, database design and implementation technology framework of FCRMS. Practice showed that using RBAC model to solve the rights management in FCRMS could achieve good effect in practical application.

Key words: RBAC model; rights management; Cadres Fulfillment Responsibilities Management System

近年来，随着和谐铁路的快速发展，铁路企业对安全管理的要求越来越高。西安铁路局依据《干部月度安全管理履责考核办法（试行）》和《新机劳〔2014〕184号》等管理和考核新机制的要求，需要构建覆盖全局各单位、各部门的西安干部履责管理信息系统（简称：西安干部履责系统），为安全管理提供技术支撑和保障。

用户权限管理功能是西安干部履责系统的重要组成部分。该系统涵盖许多业务功能，系统的用户来自不同的职能部门且数量庞大。各职能部门用户的权限各不相同，即使在相同部门，不同的用户其数据查看范围也不一样，因此有必要在用户权限管理中引入基于角色访问控制（RBAC）模型来解决实际问题。

收稿日期：2015-09-15
作者简介：关则彬，助理研究员；蒋　荟，研究员。

1　用户权限管理的业务需求概述

目前，西安干部履责系统的主要服务对象有铁路局、站段两级安全监察部门和业务部门的安全管理人员。铁路局级用户包括铁路局高层管理者、铁路局安监室人员、铁路局调度部门相关人员、铁路局业务处室相关人员；站段级用户包括站段高层管理者、站段安全科人员、站段调度部门相关人员。

系统维护方面，铁路局需要设立铁路局级劳资员，主要是每个月负责设定各个业务处和站段考核量化指标，以及初始化各个处室和站段的初始考核奖励数据。各个业务处需要设立业务处管理员，主要负责本处室人员功能及角色的授权维护。每个站段设立站段管理员及劳资员，站段管理员主要负责本站段内所有人员的系统角色功能授权，设定车间管理员等；劳资员主要负责设定本站段各个干部的

量化考核指标及初始考核奖励系数等。

业务处理方面，铁路局和站段都需要设定相关的信息员，其负责干部履责考核中的安全信息流转处理。需要建立干部日常写实录入及查询、添乘报告录入及查询、词条录入及审核等一系列与具体业务领域相关的角色。

2 基于角色访问控制（RBAC）模型

2.1 RBAC基本思想

RBAC是目前广泛应用的一种权限管理方法。2003年4月，美国国家标准化和技术委员会给出了RBAC参考模型的消息描述和功能规范[1~2]。

RBAC的基本思想是：将权限分配给角色，而不是用户，再根据用户的职责赋予一定的角色，用户根据所属的角色获得相应的权限[3~4]。用户和角色、角色和权限之间都是多对多的关系[5]。

2.2 对RBAC模型进行改进

目前西安干部履责系统中涉及到许多的铁路单位和部门，它们之间业务关系复杂。同一单位中，不同职务的人员具有不同的使用权限；而相同职务但不同单位的人员也具有不同的数据查看权限。用户还可分为全局用户和专业（指铁路中划分的车辆、机务、工务、电务、运输等）内部用户两种类型。全局用户（如系统管理员）可以操作（浏览、添加、修改、删除）所有的数据，专业用户只能对自己所在的专业部门或所管理的几个单位的数据进行操作；某些功能只有特定人员才有权使用，不同的人员即使操作相同功能，其数据权限也不相同。

根据西安干部履责系统的实际业务需要，对RBAC基本模型进行了改进，引入组织机构及层级的概念。在一定的服务、数据共享的前提下，西安干部履责系统中组织机构某个部门的用户不能访问操作另外一个同级别（或高级别）部门的数据，但允许高级别的用户访问操作低级别单位的数据。

在上述原则下，本文通过角色对功能进行分组归纳，再通过用户和角色、用户和组织机构的关系，计算出用户与功能的关系及其所对应的数据范围，如图1所示。拥有相同角色的用户，所具备的系统功能相同，但是数据范围应根据用户所属的组织机构层级来决定。

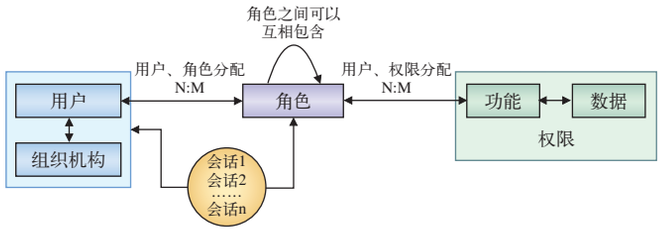

图1 改进后的RBAC模型

3 西安干部履责系统中用户权限管理的设计与实现

3.1 功能设计

根据用户需求，设计的用户权限维护子系统包括功能权限管理、角色管理、用户信息管理等主要模块，再将各个主功能模块进行细分，得到如图2所示的子系统功能模块组织。

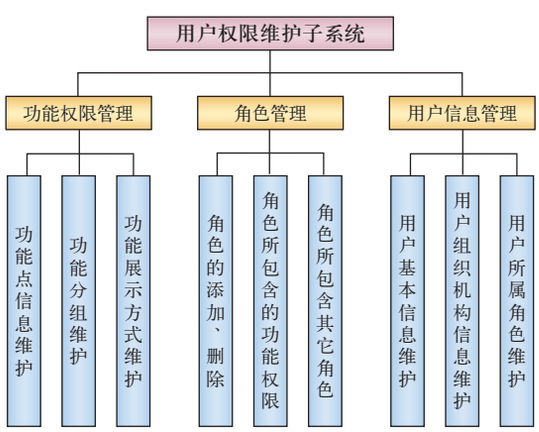

图2 功能模块图

（1）功能权限管理。该功能模块用于对西安干部履责系统中的功能进行维护，主要是定义功能的名称、功能显示方式、功能对应的界面及对功能进行分组归类。在此基础上，才能定义功能与角色的对应关系。

（2）角色管理。该功能模块用于定义西安干部履责系统中涉及的角色、角色与系统功能权限之间的对应关系。西安干部履责系统的系统管理员根据系统业务的需要，定义不同的角色，角色之间所包含的功能权限各不相同。角色与角色之间也可以有包含关系。一个角色可以被赋予多个系统用户。

（3）用户信息管理。该模块主要包括用户基本信息（姓名、职务、电话等）维护、用户组织机构及调动信息维护、用户所属角色维护等功能。一个

用户可以被授予多个角色，用户通过其所包含的角色获得相应的功能权限。

初始化西安干部履责系统时，系统只有一个超级管理员 Super。Super 通过建立铁路局级的管理员和站段级的管理员，把权限分发出去。铁路局级管理和站段级管理员可以分别维护本单位内的用户。这些管理员还可以建立子级的管理员比如车间管理员、班组管理员等来分发维护权限。

3.2 框架结构

客户端展示包括界面表示层、界面校验层和界面业务层。界面校验层用于检查用户输入的查询条件是否正确，并给出相应提示。该层主要由 Javascript 技术实现。界面业务层主要是对数据进行进一步处理，使其满足展示的需求格式。界面表示层主要将功能页面和结果页面展示给用户。界面业务层和界面展示层主要采用 ASP.Net 技术。

业务逻辑层包括数据处理业务层、数据访问业务层、数据访问中间层。数据处理业务层将满足校验条件的数据进一步处理，使其能够对数据库进行访问；将从数据库中取得的数据处理为满足条件的结果，进行展示。数据访问业务层用于实现数据访问业务，将前台方法与存储过程联系起来。数据访问中间层是连接数据业务层与数据库存储过程的桥梁，其中包含访问数据库的各种方法和属性。

数据库主要包括存储过程。存储过程直接对数据库进行访问，根据条件获取和处理数据。

具体框架结构如图 3 所示。

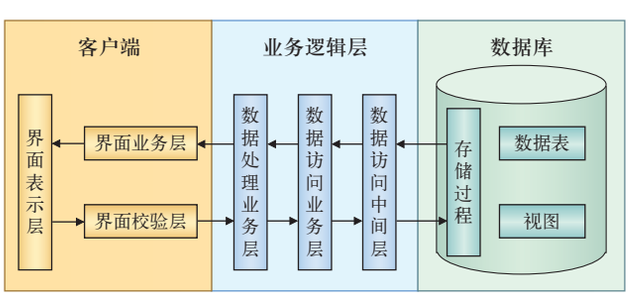

图3 框架结构图

3.3 数据库设计

基于上述模型，西安干部履责系统中权限子系统设计了如下数据表：

功能权限表（JCSJ_GNMKDM）：用于记录西安干部履责系统功能模块相关信息，包括功能名称、功能结构关系、功能对应的页面地址、功能的分组菜单等。

角色信息表（JCSJ_JSDM）：用于记录西安干部履责系统中所用到的角色的相关信息，包括角色名称、描述等。

角色关系表（JCSJ_JSDMGX）：用于记录角色与角色之间的关系。比如多个角色可以组合成一个新的角色。一个角色也可以属于多个角色。

角色功能关系表（JCSJ_JSGNGX）：用于记录功能与角色之间的对应关系。一个角色可以包含多个功能，一个功能也可以属于多个角色，它们之间是多对多的关系。

用户信息表（JCSJ_YHXX）：用于存储西安干部履责系统所有用户的基本信息，包括用户的姓名、年龄、电话、所属单位等。

组织机构表（JCSJ_ZZJG）：用于存储组织机构相关信息，包括机构名称、机构等级、机构类别、上级机构等。

用户角色关系表（JCSJ_YHJSGX）：用于存储用户所拥有的角色。用户与角色之间是多对多的关系。

数据库模型如图 4 所示。

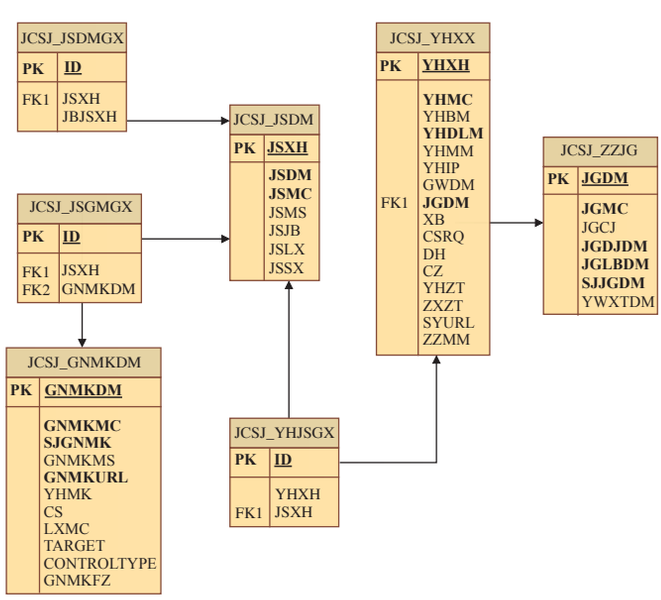

图4 数据库模型图

4 应用效果

在西安干部履责系统中引入 RBAC 模型，解决

了系统权限管理复杂性的问题。利用该模型，目前权限子系统建立了 219 个功能菜单和 167 个角色，系统用户人数达到 84 952 人，已经在全局 30 个处室和 56 个站段共 8 001 个业务部门中使用。

权限子系统初始化设定好超级用户。通过该超级用户分别建立铁路局级和站段级系统管理员。该两级的管理员再把权限分配至各自管辖范围内的用户，比如站段管理员可以建立车间管理员，实现权限逐层分解。

根据业务需求，权限子系统为铁路局高层管理者、铁路局安监室人员、铁路局调度部门相关人员、铁路局业务处室相关人员、站段高层管理者、站段安全科人员、站段调度部门相关人员都分别建立了对应的角色，并为这些角色授予一定的系统功能。

权限控制子系统的部分功能界面如图 5 ～图 7 所示。

图5　用户信息管理界面

图 5 是系统管理员为铁路局和站段的业务人员在系统中建立登录用户的界面。

图6　用户角色授权界面

图 6 是系统管理员为有效用户授予角色的界面。用户被授予角色后，就具备了角色所对应的功能。

图 7 是系统管理员维护所有角色的界面。管理员可以根据业务需要，增加相应的角色，并为该角色授予系统的某些功能。

图7　角色管理界面

5　结束语

在西安干部履责系统开发中，加入角色权限管理模块，对系统操作的安全性起到较好的保障作用，且具有较大的灵活性，实现了权限的协调转换，降低了权限管理和系统维护的复杂性。RBAC 模型的权限管理思想符合西安干部履责系统的应用要求，并能很好地适应铁路安全系统的安全策略，是一种非常重要的安全保障措施。

参考文献：

[1] 张世龙，沈玉利．一种改善 RBAC 模型用户权限获取效率的方法 [J]. 四川大学学报：自然科学版，2009, 46（1）：69-74.

[2] 付国强，陈锐皓．层次化动态权限控制模型的设计和实现 [J]. 计算机工程与设计，2007, 28（3）：690-693.

[3] 王延彬，许林英，杨海琛．OA 系统中基于角色的用户权限管理 [J]. 微处理机，2008, 8（4）：64-67.

[4] 刘建圻，曾　碧，郑秀璋．基于 RBAC 权限管理模型的改进与应用 [J]．计算机应用，2008, 28（9）：2449-2451.

[5] 严　骏，苏正烁，凌海风，等．MIS 中基于部门和角色的细粒度访问控制模型 [J]. 计算机应用，2011, 31（2）：523-526.

责任编辑　陈　蓉