

基于角色的访问控制模型在山东电网调度管理系统中的应用

山东电网调度管理系统（OMS）用户数量庞大，对于不同人员的权限控制要求比较烦琐，亟需一种行之有效的权限分配机制与策略模型应用于本管理系统，以解决目前用户权限分配细化度不足、省地县三级管理参与度欠缺等现实问题。因此，创新性地将基于岗位和角色的访问管理与控制模型应用到调度管理中，通过编制角色、用户和权限三张实体表，以及用户角色关联表、角色权限关联表两张映射表，将传统的人员、权限二维的权限管理模式，改造为人员、角色、权限三维模式，提高了开发效率，简化了权限管理，用户使用灵活方便。

辛刚¹ 李胜² 陈玉名¹ 张元鹏¹ 游大宁¹ 白鲁英^{2/1} 山东电力调度控制中心
2. 泰豪软件股份有限公司

0 引言

山东电网一体化调度生产管理系统（OMS）面向省、地、县、电厂等各级调度机构，注册用户超过16 000人，已成为山东省各级调控管理工作的重要抓手和平台。各专业信息的高度集成和访问势必要求该信息管理系统的高安全性、高可靠性、高灵活性和高延展性。既要满足各类调度机构用户的权限分配需求和一体化要求，又要分级合理限制数据共享层次和深度，有效保障调控机构信息管理的安全性和缜密性。



辛刚/高级工程师

关键词/Keywords

电力系统 ·
调度管理系统 ·
权限管理 ·
关联表 ·

1 山东电网OMS概况

2013年，国网山东省电力公司启动以“集团化运作、集约化发展、精益化管理、标准化建设”为目标的大运行体系建设。山东省地县一体化调度管理系统(OMS)作为大运行体系的重要支撑平台，于2013年1月1日正式上线。OMS

一期工程实现了山东省17个市公司、检修公司、电力科学院、98个县公司和67座统调发电厂的机构全覆盖。省调层面建设9大核心业务流程、102项业务；地调建设6大核心业务流程、61项业务；县调一期上线4个核心业务流程。共有超过15 000个用户登录系统，平均每日登录5 000~5 500人，系统整体规模和实用化水平达到国内领先。但是由于系统规模大，应用人员多，给实现安全、有序、灵活的权限管理带来了困难，在山东电网OMS系统一期运行中，主要遇到以下问题：①用户权限分配和申请/审批困难；②缺乏一致的、标准化的账号权限管理办法；③管理工作烦琐，效率低下；④账号权限变更不灵活。

在OMS二期升级改造项目中，针对以上问题进行分析解决。

2 OMS权限管理需求研究

当前主流的权限分配机制包括强制访问控制机制（Mandatory Access Control, MAC）、自主访问控制机制（Discretionary Access Control, DAC）以及基于角色的访问控制机制（Role-Based Access Control, RBAC）三类。其中，强制访问与自主访问控制机制均是采取“实施用户”与“操作权限”直接控制约束的方式进行。依托实施用户的职责级别、岗位集合、信息参与度等方面来判断对操作权限的分配原则和策略。对于用户群、权限控制菜单均稳定的应用平台尤其便利。但考虑其在实际操作中耗费较大人力，对于涉及类似省地县三

级单位且“实施用户”与“操作权限”稳固性不强的开发与应用环境而言，并不是明智之举。

相比而言，基于角色（或岗位）的访问授权机制因其高扩展性和高灵活性已经成为目前大型企业解决访问控制与授权安全的更好选择，其以“角色”的概念为支撑，并将角色作为“实施用户”与“操作权限”的传递媒介。既优化了用户与权限之间直接对话的关联耦合度，减少了人员授权引起的异动节点；又规避了由于大型企业内部结构及人员变动带来的繁琐操作过程。山东OMS权限管理按照RBAC模型设计如下。

(1) 数据对象分析

权限管理中牵扯到的数据对象包括“功能权限”、“角色”和“用户”，如图1所示。功能权限与用户之间的授权关联通过“角色”这一主线来完成，三者构建了多对多的对应关系，单个用户可以归属至多个角色组，单个角色组中可以包含多个用户；单个角色可被分配多个功能权限（或菜单），单个功能权限又可被多个角色组同时拥有。

功能权限	角色	用户
- 功能1 :	- 角色1 :	- 用户1 :
- 功能2 :	- 角色2 :	- 用户2 :
- 功能3 :	- 角色3 :	- 用户3 :
- ... :	- ... :	- ... :
- 功能n :	- 角色n :	- 用户n :

图1 授权管理数据对象

(2) 表结构分析

由于这三个对象是多对多的关系，在转换成数据库表后，需要再依托另外附加的两张数据库表来完成其关联与映射关系，即图2中的“用户角色关联表”和“角色权限关联表”，前者用于记录用户表与角色表之间的数据依存与交互，后者用于记录角色表与权限表之间的映射与交互。根据以上分析，表结构字段如图2所示。

(3) 整体结构

该系统在权限管理的数据库架构上严格定义并区分了主干基础表与数据关系表的构建，三张基础表分别记录了三类对象互不干扰的自身信

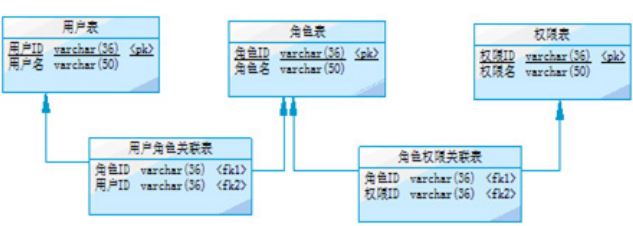


图2 表结构字段

息，两张关系表实时更新三张基础表之间的数据交互与映射。

三张基础表用于记录系统权限管理的核心要素：用户、角色和权限，三者数据库表结构稳定，推广至各类系统应用，三核心要素缺一不可，且其表数据在扩充时互不影响。

两张关系表构建并记录三张表数据之间的关联关系，在实际应用系统中，如果需要更改用户所属角色，或者变动角色组包含的权限信息，反映到该关系表，即对应修改了数据表的某条记录。

3 系统实现

3.1 权限管理

权限管理是指管理OMS系统的所有功能，包括对资源的增加、删除、修改、停用、启用。按资源所用用户级别分为省级、地级、县级、统调电厂、省地、省地县、省地县厂、地县、地县厂、县厂。对于资源的任何操作都应该有留痕功能。界面样式如图3所示。

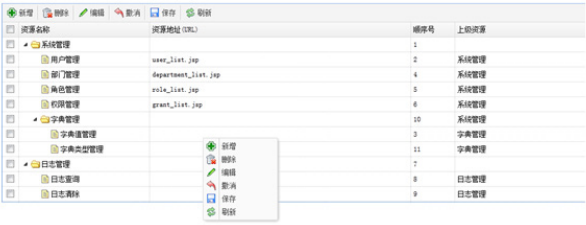


图3 权限管理界面

3.2 用户管理

用户管理是管理OMS系统中的用户，由于山东OMS系统使用人员多，为了便于管理，对人员进行分机构、分权限管理。

根据机构目录树，选择不同的机构显示不同机构下的人员。在进行用户信息维护时，用户所

属机构应该选择最细粒度，如省调的用户选择所属机构时，应该选择某一个具体的部门，如系统运行处，不能选择山东省调。

用户的维护权限应该分级管理，对于用户的维护权限应该分为省级、地级、县级、电厂（电厂分为统调电厂和地方电厂）。省级权限可以维护任何用户信息；地级权限可以维护地级、县级、电厂(包括地级地方电厂和县级地方电厂)的用户信息；县级权限可以维护县级、县级地方电厂的用户信息；电厂权限只能维护电厂用户信息。对于用户管理的任何操作都应该有留痕功能。界面样式如图4所示。

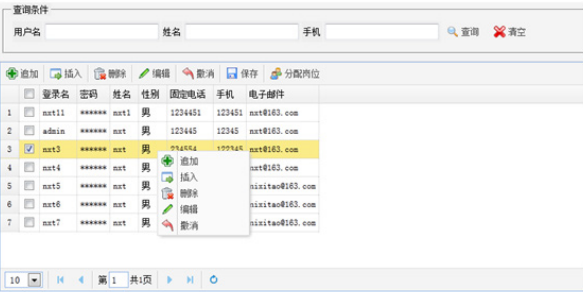


图4 用户管理界面

3.3 角色管理

角色管理又称作岗位管理，是管理OMS系统中的岗位。岗位是权限分配的单位与载体。岗位通过继承关系支持分级的权限实现。如处长岗位同时具有处长岗位、处内不同业务人员岗位。

为了便于分级管理，山东OMS系统中的岗位按组织机构进行分级，每个组织机构下面可以设置自己的岗位，岗位的维护权限应该分级管理，对于岗位的维护权限应该分为省级、地级、县级、电厂。省级权限可以维护任何岗位信息；地级权限可以维护地级、县级、地级地方电厂和县级地方电厂的岗位信息；县级权限可以维护县级、县级地方电厂的岗位信息；电厂权限只能维护电厂岗位信息。

3.4 用户与角色管理

用户与角色管理，用于记录管理系统中的实施用户和角色群组之间的联动关系和组织映射，即这个用户有哪些角色（岗位）。一个用户可以

有多个角色（岗位），一个角色（岗位）也可对应多个用户。

3.5 角色权限管理

角色（岗位）授权管理，是实现系统功能和角色（岗位）之间的关联关系映射，即这个角色（岗位）可以进行哪些操作。一个角色（岗位）可以有多个操作权限，一个操作权限也可对应多个角色（岗位）。如总工的角色（岗位）与处长的角色（岗位），总工的角色（岗位）可以有设备参数综合查询的权限，处长的角色（岗位）也可以有设备综合查询的权限；设备参数综合查询的权限即可以属于总工的角色（岗位）也可以属于处长的角色（岗位）。

对于角色（岗位）的授权的权限应该分为省级、地级、县级、电厂。省级权限可以授权任何角色（岗位）的操作权限；地级权限可以授权地级、县级、电厂的角色（岗位）的操作权限；县级权限可以授权县级、电厂的角色（岗位）的操作权限；电厂权限只能授权电厂角色（岗位）的操作权限。

3.6 系统创新

传统的权限管理基本上都是用户→岗位→权限或者用户→岗位组→岗位→权限的方式，但如果一个人的岗位过多或者一个系统中有成百上千个岗位，如果给某个人的取消一个新权限时，首先要找到这个人所属的岗位，由于这个人的岗位很多，就必须查阅系统维护的所有岗位，给系统维护人员造成非常大的工作量。为解决此问题，应该将某人的岗位直观地显示出所对应的权限，这样就很直观地找到该权限所在的岗位，并且在该岗位上取消相应的权限，如图5所示。

4 结束语

本文基于RBAC模式开展系统权限管理，通过编制角色、用户和权限三张实体表，和用户角色关联表、角色权限关联表两张映射表，完善解决了“角色”概念引入后对系统的影响。在实际应用过程中，用户一致反映符合调控系统的业务需求，使用灵活方便，满足了山东电网调度OMS用户量大、安全防护等级高等需求，具有重要的推

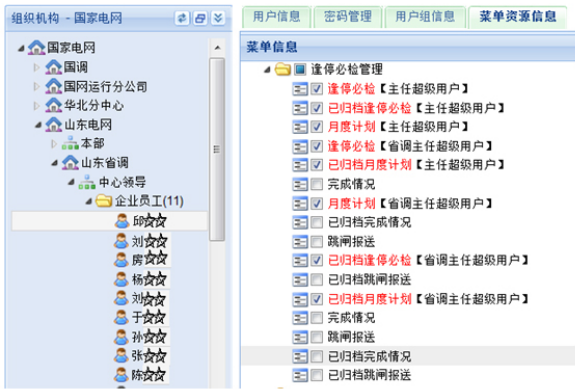


图5 人员权限综合管理页面

广应用价值。

参考文献

[1] 刘晓娟. 省地县一体化电力调度管理系统通用权限方案[D]. 大连: 大连理工大学, 2013.

(收稿日期: 2015-12-10) **EA**

(编辑: 鞠佳)

(上接第611页)

能^[6-7]。存储的历史数据可依据时间显示图表曲线, 提供元器件异常点分析, 元器件寿命推测分析。依托天津市电力公司, 实时实地对该系统进行了试运行。

5 结束语

综上所述, 使用温度、振动、烟雾三大指标, 通过3G无线通信建立整体监控网络, 对智能变电站二次设备的状态进行综合全面的实时监控, 既解决现有无线局域网通信的局限性, 也解决单一监测指标的片面性。在二次设备的状态监控历史数据的基础上, 通过深入挖掘及综合分析, 最终为检修维护人员使用和管理二次设备, 智能判断和评估保护设备健康状况, 快速分析和处理电网事故, 提供实用的数据参考和技术支持, 从而减少专业人员运维的工作量, 提高智能站继电保护的可靠性, 有远大前景和重要意义。

参考文献

[1] 王阳光, 尹项根, 游大海, 等. 应用于变电站自动化系统的无线传感器网络技术[J]. 电网技术,

[2] 李伟, 郭登峰, 徐正, 等. 基于R3方法论的企业级统一角色权限管理在电力企业中的运用[J]. 山电力信息化, 2010, 8(7).

[3] 靳丹, 张小东, 刘少博, 等. 电力企业统一权限管理系统的研究与应用[J]. 电力信息化, 2010, 8(7).

[4] 朱建江, 王宁生, 等. 一种通用的应用系统权限管理的实现方法[J]. 计算机应用研究, 2001, 18(7): 62-63.

作者简介

辛刚 (1971-), 男, 高级工程师, 主要从事电网调度运行与控制、电网调度安全管理、新能源并网与运行、电网调度综合技术管理方面的工作。

(收稿日期: 2015-12-10) **EA**

(编辑: 鞠佳)

2009(2).

[2] 刘宇通. 电子元器件的失效机理和常见故障分析[J]. 数字通信, 2012(3).

[3] 李小博, 黄新波, 陈绍英, 等. 基于ZigBee网络的智能变电站设备温度综合监测系统[J]. 高压电器, 2011(8).

[4] 谢伟红, 章健军. 3G无线传感器网络在智能配电网的应用研究[J]. 电信科学, 2010(10).

[5] 韩学军, 刘宾涛, 陈永辉, 等. 基于无线通信的高压断路器温度在线监测系统[J]. 电力系统自动化, 2006(8).

[6] 黄新波, 程荣贵, 王孝敬, 等. 输电线路在线监测与故障诊断[M]. 北京: 中国电力出版社, 2008.

[7] 黄新波. 变电设备在线监测与故障诊断[M]. 北京: 中国电力出版社, 2008.

作者简介

王洋 (1983-), 男, 工程师, 主要从事电力系统继电保护方面的工作。

(收稿日期: 2015-12-10) **EA**

(编辑: 鞠佳)