第29卷第6期 同济大学学报 Vol. 29 No. 6
2001年6月 JOURNAL OF TONGJI UNIVERSITY Jun. 2001

# 建设项目投资控制信息系统安全性分析与设计

王广斌

(同济大学 工程管理研究所,上海 200092)

**摘要**: 在综合分析工程项目投资控制需求和特点的基础上,结合信息处理技术的基本理论,对工程项目投资控制信息系统的安全性能进行了深入的分析和探讨,提出了信息系统的安全性模型,并在系统设计中得到了较好的应用

**关键词**: 工程项目; 投资控制; 信息系统; 安全保密性模型
**中图分类号**: F 224.13;TP 311.133.1 **文献标识码**: A **文章编号**: 0253-374X(2001)06-0747-05

# Safety Model Analysis and Design of Project Cost Control System

*WANG Guang-bin*

(Research Institute of Project Administration and Management, Tongji University, Shanghai 200092, China)

**Abstract**: The safety and secrecy of the data and system is an important and difficult field in design and development of the Project Cost Control System(PCCS). There is no solution now. Based on the theory of Project Cost Control and Information Technology, the paper discusses and analyses deeply the safety and secrecy of the data and system of the PCCS, and puts forward the safety and secrecy model PCCS which is well used in the system.

**Key words**: construction project; cost control; information system; safety and secrecy model

在建设项目投资控制信息系统中,投资数据的安全性和整个信息系统的安全设计是整个系统设计开发中十分重要和关键的内容[1].建设项目的许多投资数据是高度机密的,业主和开发商不想让外界了解或查询,当然更不允许非法用户对数据擅自修改,另一方面,工程建设过程中多个单位、多个部门、多方人员对工程建设的投资数据又需要经常广泛地接触,对于从事多个项目开发和建设的业主和从事多个项目管理的工程资询单位,其系统的项目投资数据的安全性设计和管理显得更为重要.虽然信息处理技术和数据库安全技术已经发展得十分成熟,但从项目管理和投资控制的方面来讲目前还没有较成熟的模型.本文结合工程建设的实践和惯例以及工程项目投资控制的理论,分析提出了一个全面的投资控制系统安全性保密模型.该模型在实践中获得较好的应用.

## 1 投资控制系统的安全性分析

投资控制系统的安全性包括两方面含义:一是指从信息处理技术角度来保护数据库以防止系统内数据遭到突发性破坏;二是指数据库模型的设计,既要满足项目管理和投资控制功能需要,又要防止项目投资数据被不合法用户使用.

收稿日期:2000-09-01
作者简介:王广斌(1967-),男,山东鄄城人,副教授,工学博士.

在项目管理和投资控制方面,投资控制系统的安全性需求应包括以下两点:

(1) 投资控制系统的安全保密设计应与整个企业投资控制的组织结构和管理层次的划分相适应,即要考虑企业管理的要求.企业管理的组织管理模式都具有层次性,如决策层、管理层、实施层等,每一层次所允许接触的信息和对信息所做的处理是不同的.在一个项目管理咨询公司中,某一项目组的人员应只允许接触本项目的投资数据,不能接触与自己无关项目的数据;一个部门只能接触与本部门有关的项目数据;而企业的决策者则必须接触企业内部所有项目的数据.投资控制系统的安全保密设计必须满足这一要求,具有相应的层次性.

(2) 投资控制系统的安全保密性设计应考虑对每一用户的权限进行限制和定义.系统除对每一用户允许接触的项目进行限制外,还包括对允许接触项目的那些投资数据(估算、概算、预算、标底、合同、投资使用计划、实际投资支付以及计划资金投入和实际资金投入等)和对这些数据可以进行哪些处理(仅读或又可修改又可读)进行限制和定义,如项目的标底和合同价数据不允许许多人了解,实际投资支付不允许修改,决策者的权限规定只允许看不允许读等等.投资控制系统的系统管理员须对每一用户进行登录和权限定义.

从数据库管理技术角度讲,建设项目投资控制信息系统的安全性需考虑以下因素:系统遭破坏后应可重建;为防止人为破坏,系统应能对用户进行有效地识别;为及时发现错误,系统对使用者的活动应该是可监测的.

## 2 投资控制系统的安全性模型

### 2.1 有关概念

为建立投资控制系统安全性模型,首先对模型中有关的几个概念作出说明.

#### 2.1.1 用户组

用户组就是权限基本相同的用户的集合,一个组可以包括多个用户.组的概念是对投资控制系统的安全保密设计进行结构分层次的一个重要概念,组可以是企业内部一个项目班子(接触该项目的数据),也可以是一个部门(接触该部门的数据),从投资控制系统安全保密角度来讲,它是同一个"层次"用户的集合,在一个用户组中各用户的权限可以不同.系统管理员应主要针对"组"来进行安全管理,其主要任务就是进行用户组的划分并进行相应的维护和管理.

#### 2.1.2 用户

用户就是享有一定权限,可进入投资控制系统的人员.在投资控制系统的安全保密设计中,每一个用户都隶属于相应的组,它拥有所在组的所有权限.一个用户可隶属于一个组,也可隶属于多个不同的组,并拥有所有这些组的权限.不同用户的权限调整应主要通过对其所属组的权限调整或归属不同的组来实现.在一个组内设组的管理员,组的管理员对组内的用户进行权限的限制和定义,用户的权限划分为三级:

(1) AD(Administration)用户——属于投资控制系统的管理员.对投资控制数据库的系统结构了解得非常清楚,负责维护和管理数据库系统,可以进行整个数据库系统的管理工作,进行软件的维护工作,并保证数据和数据库的安全,定期对数据进行备份,可以对系统中的任何数据进行修改、调整和变动.

(2) RW(Reading & Writing)用户——属于投资控制人员.可以对投资控制系统的数据进行查询、增加、修改和删除等处理.负责向系统输入并调整各个阶段的投资控制数据,进行各种数据的查询和分析工作.

(3) R(Reading)用户——属于一般用户.不能对投资控制系统的数据进行修正,只具备查询功能,并可对投资数据进行报表打印工作.

#### 2.1.3 系统管理员

系统管理员也是一个用户,系统运行中的安全保密管理由系统管理员来实现.只有具有系统管理员身份的人才能够接触到系统的安全管理功能.系统管理员可设定用户(包括其自身)的进入口令、可接触到的项目、可看到的投资数据、可接触的合同等,以及对上述对象的操作权限(只读,还是可读可写,还是全权管理).系统管理员的工作分为用户可接触对象的划分和对对象操作权限的分配两部分.

系统管理员管理工作的重点集中在"组"层上.原则上,对用户的权限分配都应集中在这一层,用户权限的变动由所在组的权限变动或加入新的组来实现;但考虑到实际操作中可能出现的具体情况,也允许进行用户层次的"微调",即针对个别用户局部调整其权限.

### 2.1.4 投资数据层

同一个项目,不同层次的用户接触投资数据的权限应该不同,如项目经理和投资控制小组领导可以接触到项目所有类型的投资数据,而低层的数据输入人员则只能涉及到其处理的那部分投资数据.根据建设项目实际情况和投资控制的要求,在投资控制信息系统中,投资数据层的安全设计所涉及的投资数据估算、概算、预算、标底、合同、投资使用计划、实际投资支付、计划资金投入和实际资金投入共计九类投资数据,与此相对应的安全级别也划分为九个级别,级别是几,该用户就只能接触到前几类投资数据.如3级用户可以接触到估算、概算、预算,而5级用户则可多接触到标底和合同价两类数据.

更进一步的考虑是投资数据可以任意组合,如用户A隶属于用户组1,用户A可进入项目1中的概算、合同价、实际投资等投资数据,这三类投资数据是任意组合的.投资数据层概念的设置就是对用户允许处理的投资数据类型进行了限制和定义.

## 2.2 投资控制系统安全保密模型

在明确以上概念的基础上,从建设项目管理和投资控制需要出发,投资控制信息系统的安全保密模型可用表1所示的一个工程项目管理咨询公司(或投资咨询公司)的数据保护案例表示[2].

在建设工程行业目前普遍采用"项目法"管理模式.设定在该公司中正从事 $n$ 个建设项目的管理(投资控制)工作,从现行普遍的公司管理角度来讲,公司相应设立 $n$ 个项目组,对投资控制信息系统而言,系统管理员(AD)在系统内相应将公司人员(用户)可设置成 $n+1$ 个用户组.$n$ 个用户组与 $n$ 个项目组对应,每一用户组只能接触每一项目数据;第 $n+1$ 个用户组可对应公司的管理层人员,其有权限看各项目投资数据,但无法进行修改和增加.对每个用户的权限由系统管理员进行设定,确定每一用户可接触到哪一类投资数据,可进行哪种权限的操作.

**表1 投资控制系统安全保密模型案例**

**Tab.1 Safety and secrecy model case of the project cost information system**

| 项目 | 几类投资数据 | 用户组1 | | | … | 用户组2 | | | … | … | 用户组 $n$ | 用户组 $n+1$ | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | A | B | C | … | H | I | J | … | … | … | X | Y |
| 工程项目1 | 1 估算 | R | R | RW | … | | | | | … | … | R | R |
| | 2 概算 | R | R | RW | … | | | | | … | … | R | R |
| | 3 预算 | R | R | RW | … | | | | | … | … | R | R |
| | 4 标底 | R | R | RW | … | | | | | … | … | R | R |
| | 5 合同价 | R | RW | R | … | | | | | … | … | R | R |
| | 6 资金投入计划 | R | RW | R | … | | | | | … | … | R | R |
| | 7 计划资金投入 | R | RW | R | | | | | | | | R | R |
| | 8 实际资金投入 | R | RW | R | | | | | | | | R | R |
| | 9 实际投资 | R | RW | R | … | | | | | … | … | R | R |
| 工程项目2 | 1 估算 | | | | … | R | R | RW | | … | … | R | R |
| | 2 概算 | | | | … | R | R | RW | | … | … | R | R |
| | 3 预算 | | | | … | R | R | RW | | … | … | R | R |
| | 4 标底 | | | | … | R | R | RW | | … | … | R | R |
| | 5 合同价 | | | | … | R | RW | RW | | … | … | R | R |
| | 6 资金投入计划 | | | | … | R | RW | RW | | … | … | R | R |
| | 7 计划资金投入 | | | | | R | RW | RW | | | | R | R |
| | 8 实际资金投入 | | | | | R | RW | RW | | | | R | R |
| | 9 实际投资 | | | | … | R | R | RW | | … | … | R | R |
| … | …… | | | | | | | | | … | … | … | … |
| 工程项目n | …… | … | … | … | … | … | … | … | … | … | … | R | R |

注:表中R表示可读该项目数据,RW表示可读写该项目数据.

表1中用户与公司中对应职位人员可根据公司管理组织结构和项目管理的具体情况进行确定，一般而言，公司中管理人员和表1中用户的对应关系可按表2进行定义.

表2 安全保密模型中用户与公司中对应职位人员表

Tab.2 Map of the users and the company position in the case model

| 序号 | 用户组/用户 | 对应职位或人员 | 备 注 |
|---|---|---|---|
| 1 | 第 $n+1$ 用户组/X,Y | 总经理,总经济师等 | 可读所有项目数据 |
| 2 | 用户组1/A | 第一项目部经理 | 可读项目1数据 |
| 3 | 用户组1/B,C | 第一项目部投资控制人员 | 可读写有关项目1数据 |
| 4 | 用户组2/H | 第二项目部经理 | 可读项目2数据 |
| 5 | 用户组2/I,J | 第二项目部投资控制人员 | 可读写有关项目2数据 |

从上述分析可以看出，投资控制系统安全策略的实现是逐层深入进行的.整个安全保密模型是一个二维表，这一模型满足了安全保密的功能要求，体现了数据安全保密的层次性(见图1).

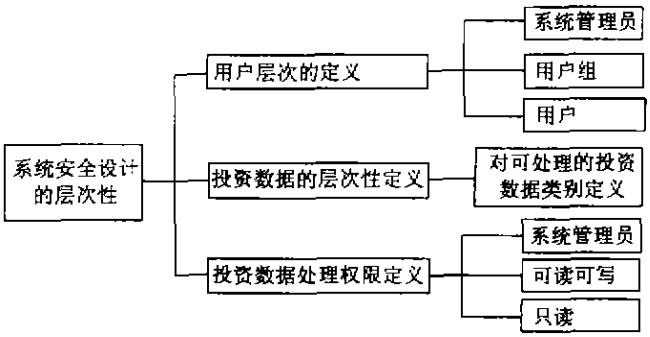


图1 投资控制系统安全保密模型的层次性

Fig.1 Hierarchism of the safety and secrecy model

## 3 信息系统的安全设计和管理

除了以上安全保密模型外，工程项目投资控制信息系统的数据和系统的安全保密还应十分重视应用数据库的恢复和安全性等技术.这涉及到一个十分重要的问题就是数据库管理系统的选择和确定.根据作者参与设计的三个有关投资控制系统(两个为特定用户开发，一个为产品开发)的经验，小型的数据库系统如Foxpro,Access难以满足系统在安全上的要求，大型的数据库管理系统如Oracle,Sybase,Informix,DB2等则有相当的优越性.在作者参与设计开发的工程项目投资控制软件(DP-1/CC)中后台采用了Oracle DBMS(VER7.1)，前台采用Oracle Develper 2000，其数据的安全保密方面主要注意了以下几方面的分析设计：

(1) 应用Oracle中的数据转储技术和登记日记技术以设计和实现投资数据在遭破坏后数据的恢复与重建.Oracle向DBA提供了多种转储后备副本(如COPY,EXPORT,SPOOL等)和相应的多种重装后备副本方法(COPY,IMPORT,LOADER等)；在登记日记技术方面，Oracle 7提供了REDO日志文件和回滚段(Rollback Segment)技术[3]；

(2) 应用Oracle DBMS中数据锁(DML)和字典锁(包括语法分析锁和DDL锁)技术实现对投资控制信息系统多用户环境下的并发控制，保证数据的一致性；

(3) 根据以上设计的投资控制信息系统安全保密模型，应用Oracle DBMS的用户标识和签定机制、授权与检查机制实现用户对系统与数据库对象权限分层次的定义和存取控制(包括自主存取控制DAC和强制存取控制MAC)；

(4) 应用Oracle DBMS的用户级审计和系统级审计技术，实现对用户访问的记录监控，并应用数据库触发器定义技术实现对非法用户的监控和报警功能[4].

Oracle DBMS提供了多种安全性措施和安全性检查，其安全性机制与操作系统的安全机制彼此独立，其中Oracle的数据字典在其安全性授权和检查以及审计技术中起着重要作用.此外，对投资控制信息系统中高度敏感的数据，如工程项目的标底价、合同价等机密数据，还可考虑采用特殊的数据加密，如DES密钥加密技术等.

另一方面，系统的安全性还必须考虑系统的管理安全问题，包括：建立严格的投资控制系统的工作制度，投资控制人员要根据有关的工作条例，严守工作机密等.

## 4 结语

在作者参与设计开发的工程项目投资控制软件(DP-1/CC)(在 Windows NT,Unix 环境开发)中采用了以上分析设计的安全保密模型,该信息系统软件经过在长江口一水利交通项目(总投资约 150 亿人民币,建设期 10 年)和上海浦东的高层房地产项目(两栋联体 30 层的外销高标准商住楼,总投资约一亿美元)等实际工程中的应用和多次与有关投资控制实际工作人员的探讨和分析,证明本模型能较好地满足工程项目投资控制和企业管理的需要,取得了较好的应用成果.

**参考文献:**

[1] Eidlin N N Cost control system for PMT use[A]. AACE Transactions[C]. Morgantown:AACE International,1989. CSC 6.

[2] 同济大学建设监理研究所,Infoage Systems Corporation Ltd. 计算机辅助投资控制系统(DP-1/CC)手册和设计文档[R] 上海:同济大学工程管理研究所,1998.

[3] Barker R CASE'METHOD:task and deliverables[M] London:Oracle Corporation U K Ltd,1990.

[4] Seibert G H. Oracle data processing a manager's handbook[M] New York:Mc Graw-Hill Inc,1993.

·下期文章摘要预报·

### 土-桩-结构相互作用体系的振动台模型试验

楼梦麟,王文剑,马恒春,朱　彤

通过土-桩-结构体系的振动台模型试验,探讨了土-结构相互作用对结构动力特性和结构地震反应的影响.试验结果表明,土-结构相互作用使结构体系的自振频率降低,使体系的阻尼大大增加.土-结构相互作用还使结构顶部的加速度反应和结构底部的应变反应减小.

### 变厚度开顶扁球壳大挠度理论的改进多重尺度法

康盛亮

综合利用近代分析和多重尺度法,讨论了大几何参数的变厚度开顶扁球壳,在内边缘集中线布荷载,外边缘均布力矩作用下的非线性屈曲问题;求得了扁薄壳几何参数 $k$ 值较大时这一问题的一致有效的渐近解;分析了集中激励引起的边界层效应和响应问题.