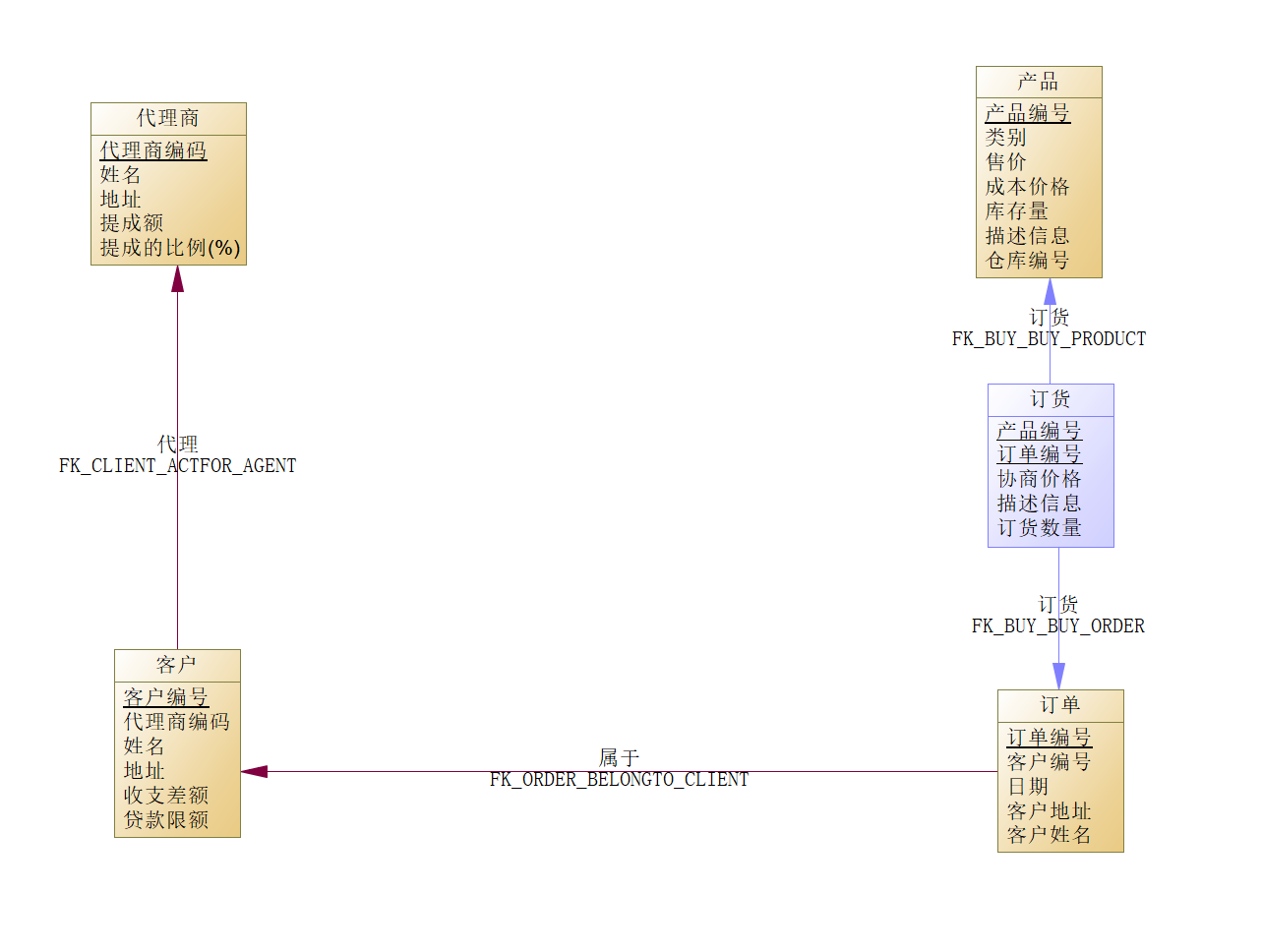
工厂信息处理系统数据库完整性和安全性的设计

**一、数据库结构说明**

**1.工厂信息处理系统PDM:**



**2.数据表说明：**

**Agent(代理商)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 中文含义 | 类型 | 可否空 | 备注 |
| Aqnum | 代理商编号 | CHAR(7) | N | 主码PK |
| Agname | 名称 | VARCHAR(20) | N | 主码PK |
| Agaddress | 地址 | VARCHAR(100) | Y |  |
| Pushmoney | 提成额 | FLOAT(10) | Y | 大于0 |
| Pmpercent | 提成比例 | INTEGAR | Y | 取值区间(0,100) |

**Client(客户)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 中文含义 | 类型 | 可否空 | 备注 |
| Clinum | 客户编号 | CHAR(7) | N | 主码PK |
| Agnum | 代理商编号 | CHAR(7) | N | 外码FK，引用自Agent表的代理商编号 |
| Cliname | 名称 | VARCHAR(20) | N |  |
| Address | 地址 | VARCHAR(100) | Y |  |
| Paybalance | 收支差额 | FLOAT(10) | Y | 大于等于0 |
| Maxcredit | 贷款限额 | FLOAT(10 | Y | 大于0 |

**Buy(订货)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 中文含义 | 类型 | 可否空 | 备注 |
| Pronum | 产品编号 | CHAR(6) | N | 和订单编号构成主码PK |
| Ordnum | 订单编号 | CHAR(6) | N | 和产品编号构成主码PK |
| Negoprice | 协商价格 | FLOAT(10) | Y | 大于总成本价 |
| Info | 额外信息 | VARCHAR(100) | Y |  |
| Amount | 购买数量 | INTEGAR | Y | 大于0 |

**Order(订单)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 中文含义 | 类型 | 可否空 | 备注 |
| Ordnum | 编号 | CHAR(6) | N | 主码PK |
| Clinum | 客户编号 | CHAR(7) | N | 外码FK,引用自客户表的客户编号 |
| Date | 日期 | DATE | N | 格式：  YYYY-MM-DD |

**Product(产品)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 中文含义 | 类型 | 可否空 | 备注 |
| Pronum | 编号 | VARCHAR(6) | N | 主码PK |
| Proclass | 类别 | VARCHAR(10) | Y |  |
| Price | 价格 | INTEGAR | Y | 大于成本 |
| Costs | 成本 | INTEGAR | Y | 大于0 |
| Storages | 库存数量 | INTEGAR | Y | 大于等于0 |
| Proinfo | 信息 | VARCHAR(100) | Y |  |
| Warenum | 仓库编号 | VARCHAR(5) | N | 不能取“00000” |

**二、数据库安全性方案设计**

**1.用户标识和鉴别**

**（1）角色定义**

超级管理员 - 拥有访问所有数据和执行所有操作的权限。

代理商 - 只能访问与其相关的客户和订单信息，以及查看自己的提成信息。

客户 - 只能查看自己的订单信息和收支差额、欠款限额。

产品管理员 - 负责管理产品信息，包括库存和价格。

订单处理员 - 负责处理订单，包括创建和修改订单。

**（2）用户鉴别：**

**I.用户名和密码:** 每个用户必须使用唯一的用户名和强密码进行身份验证。

**II.多因素认证 (MFA):** 增加一个额外的安全层，通过需要第二种验证方式（例如，发送到用户移动设备的代码）进行身份验证。

2.访问控制

超级管理员：

可以访问所有视图和执行所有数据库操作。

代理商：

只能访问代理商视图，不能修改数据。

客户：

只能访问客户视图，不能修改数据。

产品管理员：

可以访问产品管理员视图，可以添加、修改和删除产品信息。

订单处理员：

可以访问订单处理员视图，可以创建和修改订单信息。

**3. 强制访问控制方法**

**（1）数据分类和标签:**

敏感数据: 包含客户信息和代理商信息的字段（如 Clinum, Agnum, Cliname, Agname）。

一般数据: 其他非敏感字段。

**（2）强制访问控制:**

只有具有适当权限的角色（如管理员）可以访问敏感数据。

对敏感数据进行读/写操作时，需进行严格的权限检查。

**4. 视图和查询修改**

代理商视图

代理商客户信息：客户编号，姓名，地址，收支差额，欠款限额。

代理商订单信息：订单编号，日期，客户姓名。

客户视图

客户订单信息：订单编号，日期，代理商姓名，地址。

客户信息：客户编号，姓名，地址，欠款限额。

订单处理员视图

订货信息：订单编号，产品编号，描述信息，订货数量，协商价格。

**5. 跟踪审计**

**（1）审计日志:**

记录所有对数据库的访问和修改操作。

审计日志应包含以下信息：用户ID、操作时间、操作类型（如查询、插入、更新、删除）、操作对象（如表名、字段名）、操作结果。

**（2）定期审计:**

定期检查审计日志，确保没有异常行为或未经授权的访问。

**6. 数据加密**

**（1）静态数据加密:**

对数据库中的敏感数据进行加密存储（如客户信息、代理商信息）。

**（2）传输数据加密:**

使用SSL/TLS加密传输过程中数据，确保数据在网络传输中不被窃取。

**（3）加密管理:**

使用强加密算法（如AES-256）。

定期更新加密密钥，并对旧密钥进行安全销毁。

**三、openGauss数据库脚本代码**

**/\*\*角色定义/**

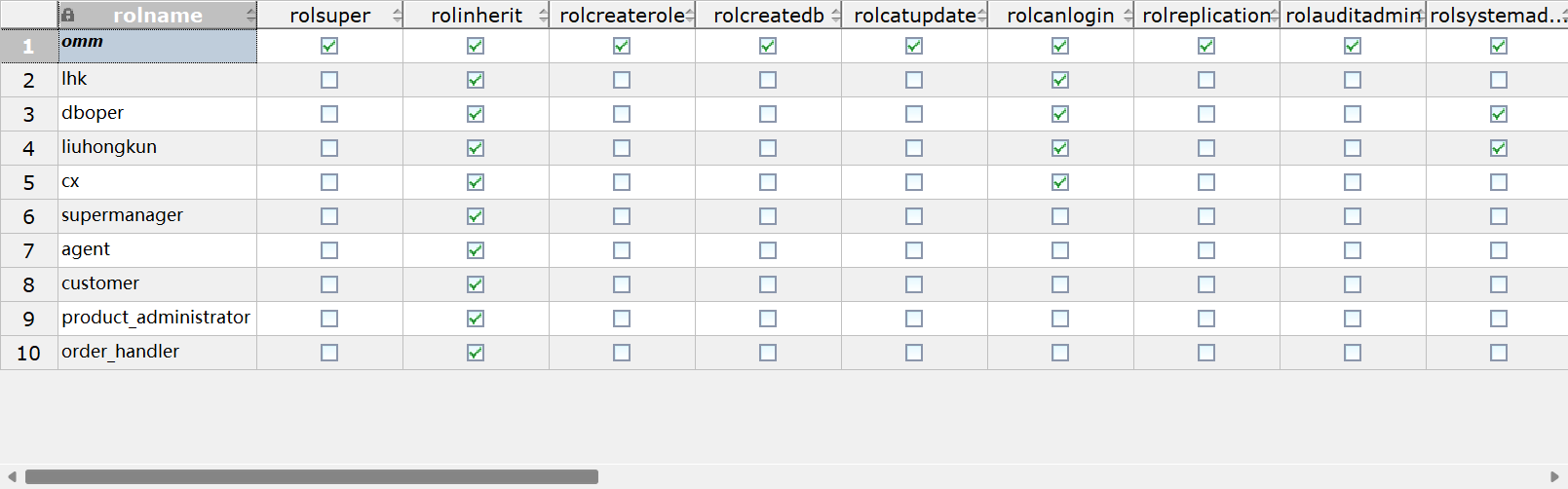
CREATE ROLE supermanager IDENTIFIED BY 'liuhongkun@123';

CREATE ROLE agent IDENTIFIED BY 'liuhongkun@123';

CREATE ROLE customer IDENTIFIED BY 'liuhongkun@123';

CREATE ROLE product\_administrator IDENTIFIED BY 'liuhongkun@123';

CREATE ROLE order\_handler IDENTIFIED BY 'liuhongkun@123';



/\*角色权限设计\*/

/\*超级管理员\*/

ALTER ROLE supermanager SYSADMIN;

/\*代理商\*/

GRANT USAGE ON SCHEMA liuhongkun TO agent;

GRANT SELECT ON liuhongkun.AgentView TO agent;

/\*客户\*/

GRANT USAGE ON SCHEMA liuhongkun TO client;

GRANT SELECT ON liuhongkun.ClientView TO client;

/\*产品管理员\*/

GRANT SELECT, INSERT, UPDATE, DELETE ON liuhongkun.product TO

product\_administrator;

GRANT USAGE ON SCHEMA liuhongkun TO product\_administrator;

/\*订单处理员\*/

GRANT SELECT, INSERT, UPDATE ON liuhongkun."Order" TO order\_handler;

GRANT USAGE ON SCHEMA liuhongkun TO order\_handler;

/\*代理商视图\*/

CREATE VIEW AgentView AS

SELECT agname, agaddress, agnum, pmpercent, pushmoney

FROM agent;

/\*客户视图\*/

CREATE VIEW ClientView AS

SELECT cliname, address, clinum, agnum, maxcredit, paybalance

FROM client;

/\*订单处理员视图\*/

CREATE VIEW OrderHandlerView AS

SELECT

o.ordnum,

o.date,

c.cliname,

c.address

FROM

"Order" o

JOIN

Client c ON o.clinum = c.clinum;

**四、数据库设计遇到的问题及体会**

**1.遇到的问题**

(1)数据一致性和约束的定义：

如何确保各个表之间的数据一致性，例如代理商编号（Agnum）在Client表和Agent表中的一致性。

如何定义和实现数据约束，如提成比例（Pmpercent）的取值范围、贷款限额（Maxcredit）的最大值限制等。

(2)角色和权限的设计：

如何合理地分配角色和权限，确保不同用户只能访问和操作与其角色相关的数据。

在设计视图时，确保视图的定义能满足不同角色的业务需求，同时保证数据的安全性。

(3)视图的设计：

如何设计合适的视图，使得用户在访问数据时能够简化操作，并且只看到自己权限内的数据。

确保视图的定义能够适应业务需求的变化，具有一定的灵活性。

**2.体会**

(1) 在设计数据库结构时，数据一致性是非常重要的。通过合理的主键、外键约束和数据类型的选择，可以有效地保证数据的一致性和完整性。

例如，通过在Client表中定义Agnum作为外键，可以确保每个客户都关联到一个合法的代理商。

(2)角色和权限的设计需要结合业务需求，进行精细化管理，确保系统的安全性和易用性。

通过为不同角色创建不同的视图，可以限制用户只能访问和操作与其角色相关的数据，提高系统的安全性。

(3)视图是数据库设计中的重要工具，通过合理设计视图，可以简化用户操作，提高数据访问的安全性和效率。

例如，通过为代理商、客户和订单处理员分别设计视图，可以确保他们只能访问和操作与其角色相关的数据，同时简化了数据查询操作。