**银联风险管理系统**

1. 银联二代系统整体架构 3

1.1. 银联二代系统业务架构 3

1.2. 银联二代系统技术架构 3

2. 风险管理系统在二代系统中的位置 4

2.1. 风险管理业务定位与规划 4

2.2. 风险管理系统与其他业务系统接口 5

3. 风险管理系统整体架构 10

3.1. 概述 10

3.1.1. 二代风险管理系统整体业务架构 10

3.1.2. 二代风险管理系统主要功能 10

3.1.3. 二代风险管理系统功能模块详解 11

3.2. 管理子系统 12

3.2.1. 功能简介 12

3.2.2. 功能详解 12

3.3. 服务子系统 14

3.3.1. 功能说明 14

3.3.2. 实现机制 16

3.3.3. 服务划分 17

3.4. 批量子系统 18

3.4.1. 功能说明 18

3.4.2. 实现机制 19

3.5. 准实时子系统 21

3.5.1. 功能说明 21

3.5.2. 业务流程 22

3.5.3. 实现机制 22

3.6. 实时子系统 24

3.6.1. 实时子系统业务流程 24

3.6.2. 实时系统的业务角色 24

3.6.3. 实时系统内部工作流程 25

# 银联二代系统整体架构

## 银联二代系统业务架构

第二代系统中业务服务主要由开放的转接清算系统、POS收单接入系统、多渠道接入支持系统、风险管理系统、联合营销支持系统、数据服务系统、国际业务支持系统等业务模块组成。业务逻辑和银联核心逻辑见下图。



## 银联二代系统技术架构

第二代银联系统以交易转接系统上海、北京“双中心同步运行”为核心，以收单、发卡前置和外围应用系统为依托，以网络及基础环境为保障，采用统一的技术标准、一体化运维管理的集中式系统架构。二代系统具备集中式、标准化、高可靠、松耦合、参数化设计等特点，其系统技术架构如图所示。



# 风险管理系统在二代系统中的位置

## 风险管理业务定位与规划

根据不同业务风险的性质及银联在风险中承担的组织角色，银联面临的各类业务风险可划分为直接风险和间接风险两类。

直接风险指的是银联作为独立经营机构所直接承担、面对的风险，而间接风险则是银联作为卡组织，不直接承担，但需协助成员机构、持卡人以及商户等来共同防范、应对的风险，后者的着眼点在于提升银联卡业务的安全性，提高银联品牌竞争力和美誉度。

直接风险主要包括操作（业务运营）风险、清算（信用）风险、政策风险等。间接风险主要包括信用风险、欺诈风险等。

总结归纳银联面临的主要风险如下图所示。



## 风险管理系统与其他业务系统接口

二代风险管理系统是中国银联第二代跨行交易清算系统的重要组成部分，风险系统与二代系统总体框架内各业务系统相互支持、相互补充，构成一个有机整体。

二代风险系统与其他系统间的关系主要表现在两个方面，一方面风险系统与其他业务系统之间存在各种形式的数据交换，从对方获得本方所需的业务数据；另一方面风险系统将风险分析的结果向其他业务系统输出，由相关业务系统根据结果具体执行风险控制功能。

下图是风险管理系统与其他业务系统接口总览图。



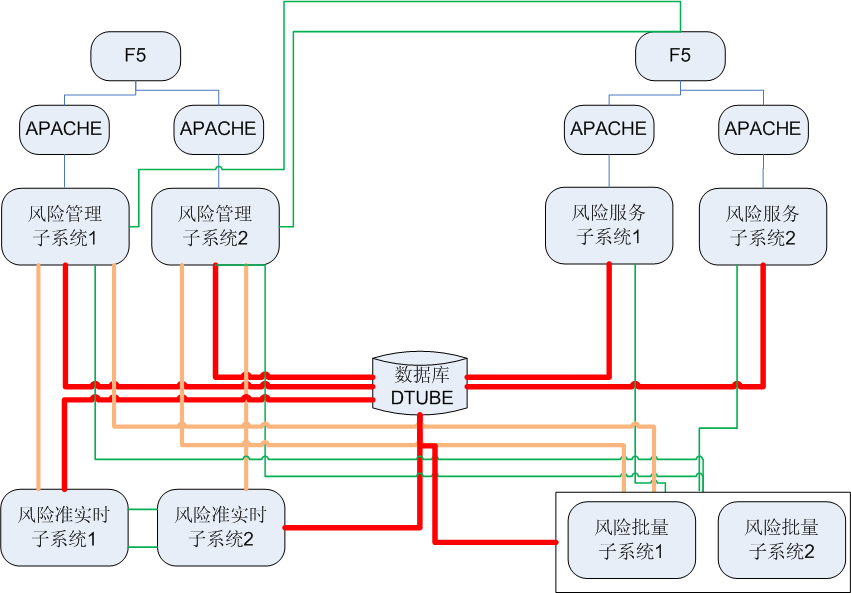
风险系统与各业务系统之间数据交换的主要内容如下表所示。具体说明如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **业务系统名称** | **输入输出** | **内容** | **说明** |
| 转 接 系 统 | 从风险系统输入 | 交易实时风险评分 | 在转接交易时，接收风险系统实时计算的交易评分，并将分值作为交易报文的一部分上送发卡机构 |
| 中止转接的机构列表 | 停止列表中机构的交易转接 |
| 向风险系统输出 | 实时交易流水 | 向风险系统实时发送交易流水 |
| 日终清算流水（含差错） | 日终向风险系统发送清算流水 |
| 基础参数（卡BIN、机构代码等） | 每日向风险系统提供基础参数信息，包括BIN表、机构代码等 |
| 清算系统 | 从风险系统输入 | 暂停清算指令（交易、卡片、商户、机构） | 根据风险系统发送的暂停清算指令，暂停指定交易、卡片、商户或机构的清算 |
| 向风险系统输出 | 大额清算系统借记指令排队数据 | 每日向风险系统提供大额清算系统借记指令排队数据 |
| 成员机构每日清算汇总数据 | 每日向风险系统提供成员机构清算金额 |
| 国际业务支持平台 | 从风险系统输入 | 暂停交易指令  （商户、卡号） | 接收风险系统提供的商户、卡号暂停交易指令，对于这些商户或卡号的交易，直接给出拒绝应答 |
| 中止交易商户列表 | 停止列表中商户的交易 |
| 中止交易卡号（卡BIN）列表 | 停止列表中卡号或卡BIN的跨境交易 |
| 卡号交易限额列表 | 根据卡号交易限额，对超限的卡号暂停交易 |
| 商户交易限额 | 接收风险系统提供的商户交易限额，对于超出当日或当笔交易限额的商户，直接给出拒绝应答 |
| 向风险系统输出 | 境外商户、终端信息 | 向风险系统提供境外受理商户、受理终端的信息，包括商户名称、商户代码、所在国家、商户类型等 |
| 多渠道平台 | 从风险系统输入 | 中止交易商户列表 | 停止列表中商户的交易转接 |
| 中止交易卡号（卡BIN）列表 | 停止列表中卡号或卡BIN的交易转接 |
| 卡号交易限额列表 | 根据卡号交易限额，对超限的卡号暂停交易 |
| 商户交易控制（单笔、当日限额等） | 根据商户交易限额，对超限的交易予以拒绝 |
| 向风险系统输出 | 商户终端信息 | 向风险系统提供多渠道受理商户、受理终端的信息 |
| 用户定制信息及辅助交易信息 | 向风险系统提供定制信息以及辅助交易信息，如卡号对应的手机号码等 |
| 收单业务处理平台 | 从风险系统输入 | 中止交易商户列表 | 停止列表中商户的交易转接 |
| 中止交易卡号（卡BIN）列表 | 停止列表中卡号或卡BIN的交易转接 |
| 卡号交易限额列表 | 根据卡号交易限额，对超限的卡号暂停交易 |
| 商户交易控制（单笔、当日限额等） | 根据商户交易限额，对超限的交易予以拒绝 |
| 向风险系统输出 | 商户终端信息 | 向风险系统提供受理商户、受理终端的信息 |
| 商户集中管理平台 | 从风险系统输入 | 高风险商户、商户风险评分/评级 | 根据商户审核信息进行风险评分/评级，供商户审批使用 |
| 向风险系统输出 | 商户入网审核信息 | 向风险系统提供商户入网审核信息 |
| 商户终端信息、终端正常拨入号码 | 所有受理商户、受理终端的信息 |
| 短信  平台 | 从风险系统输入 | 提示交易 | 发送交易提示短信 |
| 风险提示 | 发送风险提示短信 |
| 向风险系统输出 | 交易安全辅助验证 | 基于短信平台的双因素验证 |
| 呼叫  中心  门户  网站 | 从风险系统输入 | 风险事件  案件提示  安全用卡知识 | 接收风险系统提供的各类风险信息 |
| 向风险系统输出 | 风险信息  卡片止付请求  卡片限额控制请求 | 接收持卡人的卡片交易控制请求，并发送给风险系统 |
| 邮件服务器 | 从风险系统输入 | 风险事件、  案件提示  交易提示  对账单 | 接收风险系统提供的各类风险信息、合并账单等 |
| 向风险系统输出 | 风险信息 | 接收持卡人的风险相关投诉、建议、情况反映等 |
| 数据仓库 | 从风险系统输入 | 各类欺诈数据  各类风险指标数据 | 接收风险系统提供的各类欺诈数据、风险指标数据等 |
| 向风险系统输出 | 风险数据分析结果 | 向风险系统输出数据分析结果，供风险系统使用 |

# 风险管理系统整体架构

## 概述

### 二代风险管理系统整体业务架构



### 二代风险管理系统主要功能

风险管理系统，既能够满足银联和银联子公司的风险管理和服务需求，保障银联自身安全，又能够满足银联作为卡组织履行风险管理和风险服务职责需要，保障银联网络安全有序，还能够满足银联开展收单业务处理、提升持卡人忠诚度需要，提升银联品牌竞争力。

二代风险管理系统的业务功能主要由以下七块组成：

-风险信息管理与服务

-成员机构风险管理与评估

-司法协助与服务

-收单风险管理

-收单风险监控

-收单风险处理

-银联卡欺诈侦测

### 二代风险管理系统功能模块详解

**风险信息管理与服务**

风险信息管理与服务部分从满足总公司、成员机构实际需要的角度出发，实现银联总分公司、成员银行、司法机构之间各类银行卡风险信息的收集、共享、统计与发布，为各类风险分析应用及风险联合防范机制的建立打下基础。主要功能包括：风险信息共享、欺诈交易报送、风险事件报送等。

**成员机构风险管理与评估**

成员机构风险评估与动态管理部分实现银联对入网机构从加入银联网络、开展业务直至推出银联网络整个生命周期的风险评估与管理，防范成员机构可能出现的信用风险、清算风险和其他业务风险。主要功能包括：机构风险信息收集与整理、动态风险评估、清算风险监控等。

**司法协助与服务**

司法协助与服务部分从防范和打击银行卡案件的角度出发，通过向司法机关提供高效、全面的银行卡案件协查服务，帮助司法机关打击各类银行卡犯罪案件，维护银行卡产业的健康发展。主要功能包括：案件协查、案件管理。

**收单风险管理**

收单风险管理部分基于银联卡组织角色，实现对银联网络内收单机构的管理。具体包括两方面的功能：一方面实现银联对收单机构商户风险的识别与监控，督促收单机构加强对商户的管理；另一方面实现银联对所属收单机构整体收单风险状况的统计与分析，并采取相关措施对收单机构进行管理，维护银联整个受理网络的健康发展。

**收单风险监控**

收单风险监控通过设定监控规则和模型，对商户进行实时监控和准实时监控，及时发现存在套现、违规移机、伪卡集中使用等可疑行为的高风险商户或终端，提示收单机构进行调查并采取风险控制措施。在监控范围上，既包括所有直联，也包括间联商户，也包括境外商户；既包括人民币商户，也包括外卡商户。

**收单风险处理**

收单业务处理部分从满足收单机构实际业务需要的角度出发，为收单机构（含专业化服务机构）提供风险管理与服务功能，实现收单机构对商户从入网准入、到退出整个生命周期全过程的风险控制。主要包括：商户入网风险审核、商户风险评级、商户培训与检查管理、商户交易控制、商户或交易清算控制、商户风险信息管理、商户风险提示服务、商户销户管理等。

**银联卡欺诈侦测**

银联卡欺诈侦测通过运用各类监控规则或模型，对银联卡特别是银联标准卡的交易进行实时/准实时监控，帮助发卡机构及时发现欺诈、套现和其它可疑交易，最大程度地减少可能出现的欺诈损失。系统同时实现对外卡欺诈交易和巨额交易的监控。在监控范围上，既包括传统渠道交易，也包括新兴渠道交易；既包括境内交易，也包括境外交易。

## 管理子系统

### 功能简介

风险管理系统主要包括系统管理、参数管理、运维管理、准实时子系统管理、批量子系统管理、实时子系统管理、响应式批量七块功能。

### 功能详解

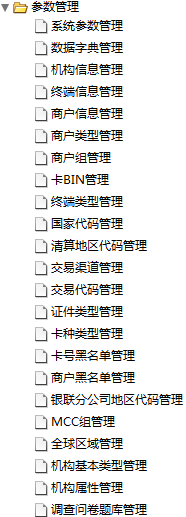
系统管理模块，主要有用户管理、角色管理、RTS管理。

用户管理主要对用户权限按机构和角色进行分配，以及密码重置等功能。

角色管理主要针对用户的角色进行维护，角色权限即为各子功能的操作权限。

RTS管理？

参数管理



系统参数管理：疑似套现处理时限配置和欺诈交易修改删除时限，单位为天。

数据字典管理：系统中用到的一些参数在该模块进行配置。

运维管理

运维管理主要包括生存状态检查、当前用户查看、审计日志管理、系统日志管理、短信发送日志管理和数据清理管理。

生存状态检查：监测风险服务子系统、风险管理子系统、批量子系统、准实时系统的运行状态。

当前用户查看：查询所有系统的用户信息。

审计日志管理：用户登录、退出系统的时间，及数据库操作信息均可查询。

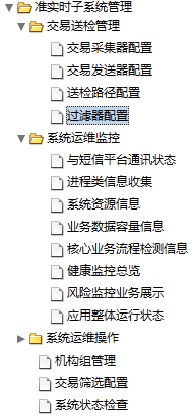
系统日志管理：四个子系统的日志查询。

短信发送日志管理：系统发送短信的时间及结果查询。

数据清理管理：设定清理周期和清理方法，定期清理特定表格的数据。

准实时子系统管理包括交易送检管理、系统运维监控、系统运维操作。

交易送检管理分交易采集器配置、交易发送器配置、送检路径配置、过滤器配置。



## 服务子系统

### 功能说明

风险服务子系统是对外部对外部用户的人机接口，是交互类的Web应用，主要实现业务上的管理、配置、监控和处理功能

通过风险服务子系统：

1. 使外部用户可以干预整个系统域的行为；
2. 使外部用户获取本系统域内的相关信息；
3. 使外部用户可以人工提交业务处理请求。

风险服务子系统主要包含以下的功能模块：

* 公告与提示
  + 公告与提示
  + 用户密码修改
* 风险信息共享
  + 风险信息查询
  + 风险信息维护
  + 风险信息权限配置
  + 风险信息查询统计
* 风险指标共享
  + 风险指标报送
  + 行业分析报告上传
  + 查询统计
* 风险事件管理
  + 风险事件报送与处理
  + 银联查询统计
  + 成员机构查询统计
* 境内欺诈交易报送
  + 检索报送
  + 批量报送
  + 疑似套现手工反馈
  + 疑似套现批量反馈
  + 已报欺诈交易维护
  + 汇总统计
* 司法协助服务
  + 案件协查
  + 案件管理
  + 司法机构协查案件查询统计
  + 成员机构案件报送查询统计
* 银行卡欺诈侦测
  + 监控模型管理
  + 业务参数管理
  + 监控结果处理
  + 发卡风险信息统计
* 虚假申请侦测
  + 虚假申请侦测参数配置
  + 虚假申请侦测
* 卡片历史交易查询
  + 卡片历史交易查询
* 收单风险管理
  + 收单风险信息查询
  + 收单风险信息统计
* 收单风险监控
  + 监控模型管理
  + 商户信息管理
  + 案例管理
  + 信息查询与下载
* 风险信息通告发布
  + 风险联系人管理
  + 风险联系人组管理
  + 风险信息通告发布
  + 风险信息通告查询
  + 查询统计
* 境外欺诈交易报送
  + 欺诈交易报送（专网）
  + 已报送欺诈交易维护
  + 查询统计报表
    - * 国家地区发卡欺诈率简表
      * 发卡机构欺诈率简表
      * 国家地区收单欺诈率简表
      * 收单机构欺诈率简表
      * 收单机构欺诈统计表-商户欺诈简表
      * 收单机构前20位MCC欺诈简表
      * 收单机构前50位商户欺诈简表
* 入网机构风险评级
  + 机构信息管理
    - * 机构信息管理
      * 机构财务信息管理
      * 措施管理
  + 机构风险信息统计查询
    - * 清算风险事件查询
      * 风险事件信息统计
      * 清算风险事件统计
  + 清算风险监控
    - * 提示联系人设置
* 商户风险评级
  + 商户入网风险评级
    - * 入网风险评级结果查询
  + 商户日常风险评级
    - * 日常不定期风险评级
      * 日常风险评级结果查询
      * 日常风险使用评级明细查询
  + 风险评级统计报告
    - * 入网风险评级统计查询
      * 日常风险评级统计查询

### 实现机制

按照风险管理系统的总体架构设计，风险服务子系统属于风险管理系统架构设计中的应用层，与Portal层及ESB进行交互，这部分内容在“系统架构设计”章节已经详细描述。在风险管理子系统内部，划分为四个层次，如下：

* 展现层

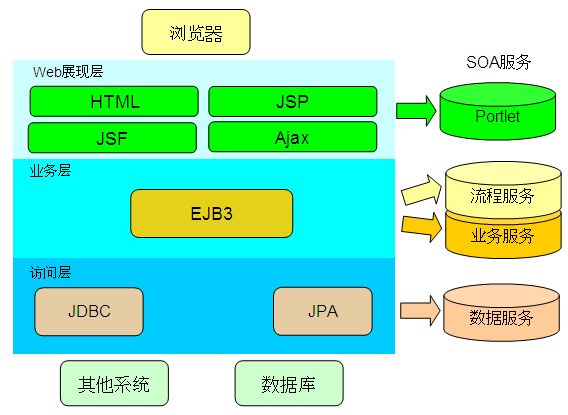
展现层，主要在这一层完成业务功能的页面展示，这一层是与Portal的接口层。

* 业务服务层

业务服务层，主要在这一层抽象出业务服务，完成业务服务的实现。这一层也是与ESB的接口层。

* 数据持久层

数据持久层，主要在这一层完成与数据库及其它系统的数据持久化服务。



各层次的具体实现方式遵照《JEE统一基础平台开发指南》的规定。

### 服务划分

在风险管理子系统的设计过程中，以服务的形式来梳理风险服务子系统的功能点。在设计过程中，将功能分为以下服务：

* 风险系统需要从ESB调用的服务
  + 风险信息共享维护反馈文件下发
  + 风险信息共享风险信息报告下发
  + 境内欺诈交易反馈文件下发
  + 境外欺诈交易反馈文件下发
* 风险系统需要注册到ESB的服务
  + 风险信息共享维护文件报送
  + 风险信息共享查询文件报送
  + 境内机构欺诈交易报送
  + 数据仓库统计量报送
  + 境外机构欺诈交易报送

## 批量子系统

### 功能说明

批量总控模块

数据采集模块

数据统计模块

收单风险侦测模块

虚假申请侦测模块

CPP侦测模块

数据清理模块

数据采集统计相关模块

侦测模块

辅助模块

商户评级模块

报表推送模块

图 5‑4风险管理系统—批量子系统功能示意图

### 实现机制

#### 批量总控

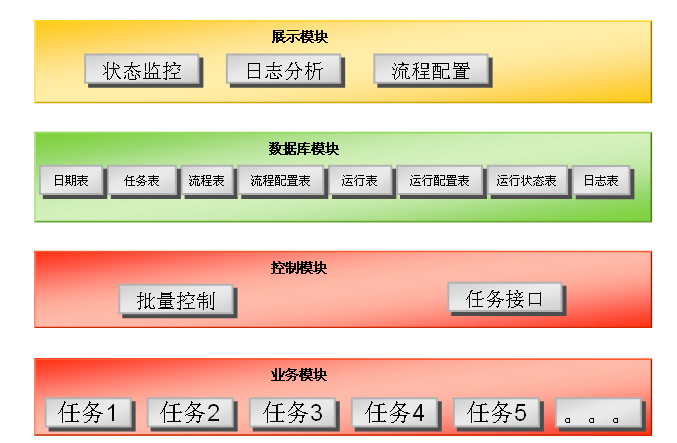


图 5‑5风险管理系统—批量总控示意图

* 批量总控设计说明

在批量总控设计中有两个概念：批量流程和批量任务

批量流程：

1．一个批量流程包含了一个或者多个批量任务。

2．一个批量流程的第一个任务由定时触发器完成。

3．一个批量流程中的任务可以是串行运行，也可以是并行运行，但不支持多个串行任务的并行。

4。一个批量流程可以设定暂停，如果一个批量流程暂停，那么当前在运行的批量任务继续运行直到结束，后续任务暂停运行。

批量流程之间可以并行运行,通过开关配置.当平行运行设为false时,按照流程设定的时间顺序执行,一个流程执行完成后下一个流程才可以启动.

5．一个批量流程不负责批量任务内部的事务处理。

6．一个批量流程中的任务可能来自不同的任务模块。

批量任务：

1．批量任务是一个业务的功能单位。

2．批量任务必须实现控制模块的任务接口。

3．批量任务内部的事务由批量任务自身实现。

批量任务应根据批量时间完成相应的任务，而不是实际时间。

4。一个批量任务可以设定取消，如果一个批量任务设定为取消，那么就不执行该批量任务。

5．一个批量任务结束后，如果不是还要重复执行的任务（如短信发送），将移除任务相应的JobDetail，以释放资源。

6．一个批量任务结束后，如果需要动态配置后面任务的启动参数，可直接修改任务执行表。

* 批量总控设计原则

展示模块、数据库模块和控制模块形成批量总控

展示模块和控制模块通过数据库进行交互

批量总控模块设计与业务隔离、可重用

流程之间应该没有依赖关系，可以并行执行

业务模块的的任务都要实现控制模块的任务接口

对于批量流程和批量任务的增删改查的生效分为两个点

对于批量流程的暂停和批量任务的取消，在流程和任务执行过程中可以生效

对于其它的修改，必须在修改后的下一个批量日生效

## 准实时子系统

### 功能说明

数据转移总控

目标表写入服务

源数据获取服务

**联机交易采集模块**

交易读取/

**交易路由分发模块**

统计量运算

可疑交易分派

规则逻辑

**风险监测主控模块**

交易发送

滞留处理

应用初始

数据清理

环境初始/应用重启

日期切换

**系统日终切换模块**

统计数据采集

涉案命

中分析

**涉案监控模块**

过滤送检

路由分发/

健康检查

交易计数

应用初始

模型装载

信息收集

**应用监控模块**

起停服务

健康与报警

信息收集xnxii

心跳检测

交易分发

交易读取

**风险库数据采集模块lyou**

交易过滤

参数加载

交易计数

应用初始

滞留处理

交易发送

参数加载

**备付金清算监控模块**

风险监控

可疑交易读取

**可疑报文通知模块**

报文组装

报文发送

短信发送服务

**分析结果处理模块**

邮件服务

图 ‑1风险管理系统—准实时子系统功能示意图

见图5-1风险管理系统—准实时子系统功能示意图，风险准实时子系统主要分为联机交易采集模块、交易路由分发模块、风险监测主控模块、应用监控模块、系统日终切换模块、涉案监控模块、风险库数据采集模块、备付金清算监控模块、分析结果处理模块。

其中联机交易采集模块、交易路由分发模块、风险监测主控模块、应用监控模块、系统日终切换模块为一期实现.图中蓝色部分为二期新增或者涉及修改的模块,红色字表示新增,红色字表示修改.

### 业务流程



风险准实时子系统在从CUPs、多渠道、外卡、国际业务等外部系统将交易流水转移到采集表后，对交易流水进行三个方面的业务分析处理：可疑（欺诈）交易侦测、司法协查监控和备付金清算风险监控。其中备付金清算风险监控和可疑交易发送报文服务属于风险二期的实施范围。

### 实现机制

风险准实时子系统设计过程可分为的四大阶段：数据采集阶段、路由分发阶段、分析处理阶段、案例分发阶段。其中，

* **数据采集阶段**实时转移外部系统的交易流水到风险系统数据库，此阶段功能在银联统一数据转移平台DTUBE框架基础上，加入风险系统的数据转移逻辑实现；
* **路由分发阶段**将交易流水转发给各子模块，此阶段功能通过交易路由分发模块实现；
* **分析处理阶段**分析可疑交易、监控涉案卡交易和备付金清算风险，此阶段功能基于银联自主产权的规则引擎和统计量引擎，通过风险检测主控模块、涉案卡监控模块和备付金风险清算模块予以实现。
* **案例分发阶段**将风险准实时系统检测到的各种风险信息和案例通知给外部系统或相关处理人员，此阶段功能通过和外部平台（例如短线平台、邮件发送平台、CUPs平台）的交互实现。

Tuxedo Server

联机交易数据库

**联机交易采集模块**

**DTUBE**

**联机交易系统**

源数据获取服务

目标表写入服务

DB2 CLI

tpacall

采集表

DB2 CLI

DB2 ESQL

**交易路由分发模块**

交易分检服务

交易发送端服务

多进程并发

消息队列

msgsnd

msgget

TCP Socket

多进程并发

**风险检测主控模块**

欺诈库

共享内存

DB2 ESQL

交易轮循

交易生成

**涉案交易监控模块**

短信交易表

**风险服务与管理子系统**

规则管理

参数管理

监控请求

数据收集服务

监控请求处理

tpforward

**应用监控模块**

WTC tpcall

tpreturn

统计量管理

规则库

JDBC

Init

分派配置

健康与报警

shmget

msgctl

模型初始

规则分析

统计量运算

可疑分派

现场输出

上下文维护

ESQL

JDBC

核心监测进程

参数装载

备付金监控

TCP Socket

**备付金清算风险监控模块**

备付金余额

ESQL

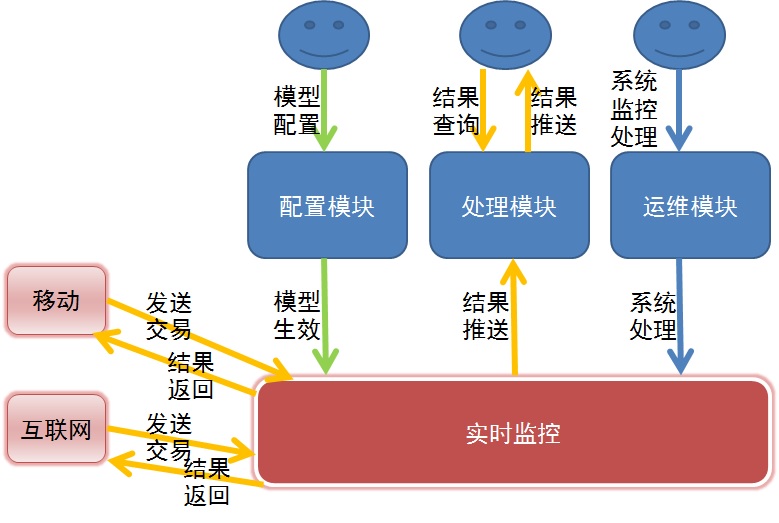
**可疑报文通知**

TCP Socket

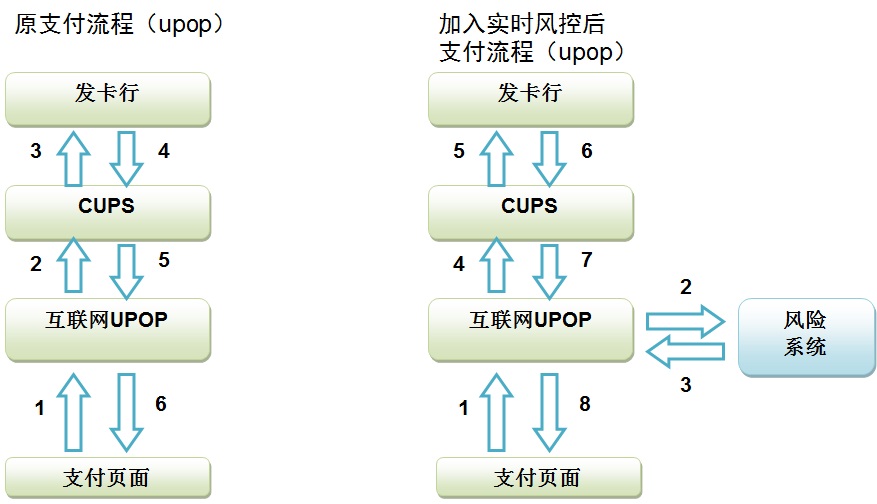
报文组装发送

## 实时子系统

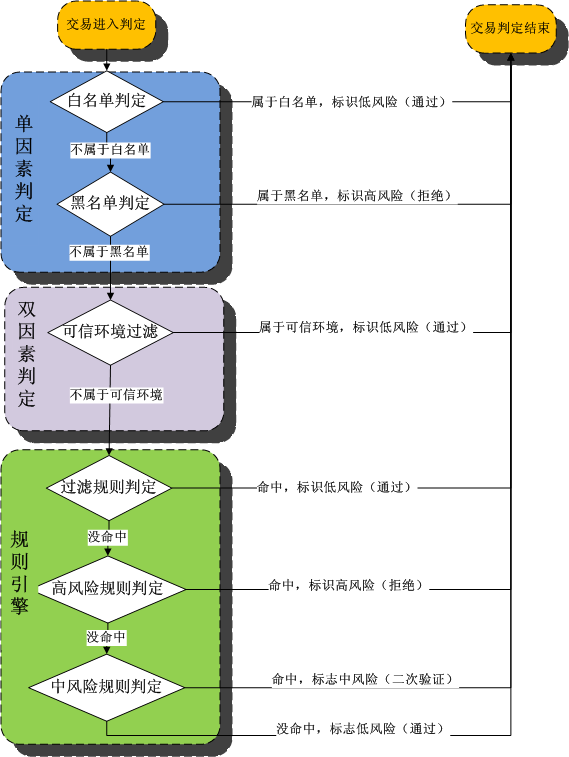
### 实时子系统业务流程



### 实时系统的业务角色



### 实时系统内部工作流程

****