

ICS 03.060

CCS A 11

团 体 标 准

T/ZQX XXXX—XXXX

期货公司异构多活交易信息系统 建设指南

Guidelines for the construction of heterogeneous multi-active trading
system in futures company

（征求意见稿）

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中国期货业协会 发布

目 次

前言.....	III
引言.....	IIIIV
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 建设目标.....	1
5 建设思路.....	2
5.1 基本原则.....	2
5.2 组织保障.....	2
5.3 基础设施.....	3
5.4 系统要求.....	3
5.5 安全合规.....	4
6 建设方案.....	4
6.1 方案选型.....	4
6.2 系统测试.....	5
6.3 系统上线.....	6
7 运行保障.....	8
7.1 业务保障.....	8
7.2 技术保障.....	8
7.3 应急方案.....	10
附录 A（资料性）案例 1：全业务异构多活建设方案.....	13
A.1 方案概述.....	13
A.2 交易多活方案.....	14
A.2.1 交易多活原理.....	14
A.2.2 交易切换流程.....	15
A.3 风控多活方案.....	15
A.4 银期多活方案.....	15
A.4.1 银期多活原理.....	15
A.4.2 银期模块部署方式.....	15
A.4.3 银期切换方案.....	16
A.5 结算多活方案.....	16
A.5.1 结算模块部署方式.....	16
A.5.2 结算流程.....	16
A.6 账户多活方案.....	16
附录 B（资料性）案例 2：核心模块异构多活建设方案.....	17

B.1 方案概述.....	17
B.2 交易多活方案.....	18
B.3 风控多活方案.....	18
B.3.1 异构系统集成风控模块.....	18
B.3.2 独立异构风控系统.....	18
参考文献.....	20

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第一部分：标准化文件的结构和起草规则》JR/T 0352.1—2026《证券期货业标准化工作导则 第1部分：标准的名称》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国期货业协会提出并归口。

本文件起草单位：XXX、XXX、XXX、XXX、XXX、XXX。

本文件主要起草人：XXX、XXX、XXX、XXX、XXX、XXX。

引 言

近年来,我国期货市场高速发展,期货公司为适应市场发展,持续加快数字化转型步伐。为提升交易信息系统的可扩展性,降低软件漏洞对业务连续性的影响,部分期货公司开始采用异构多活架构建设交易信息系统。

为指导期货公司按需开展异构多活交易信息系统建设,特制订本文件。

期货公司异构多活交易信息系统建设指南

1 范围

本文件对期货公司异构多活交易信息系统建设的目标、思路、方案进行指导，提出系统上线后运行保障关键环节的示范。

本文件适用于期货公司建设异构多活交易信息系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注明日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0059-2024 《证券期货业信息系统备份能力规范》

JR/T 0208-2021 《金融行业信息系统多活技术规范 参考架构》

JR/T 0209-2021 《金融行业信息系统多活技术规范 应用策略》

3 术语和定义

下列术语和定义适用于本文件。

3.1

异构 heterogeneous

异构指系统中包含多种不同类型、架构或技术规格的组件，这些组件在功能、性能或设计上存在显著差异，但协同工作以完成任务。常见的应用场景包括异构计算、异构网络、异构存储等。

3.2

多活 multi-active

多活是一种分布式系统架构，指多个节点同时处于活动状态，均可独立处理用户请求，并通过数据同步机制保持一致性，实现高可用与负载均衡。

4 建设目标

4.1 提升系统可用性

通过异构多活架构的容错技术，降低软件缺陷导致的技术系统风险，防范单一技术路线缺陷引发期货公司交易业务中断，提升交易信息系统的可用性。

4.2 加强容灾能力

通过构建异构多活架构，期货公司在不同地理位置部署交易中心，确保交易系统在面对各种风险，如硬件故障、软件故障、网络故障、自然灾害等情况时，异构多活交易信息系统能实现对故障交易系统的快速接管，确保交易业务“零中断”，增强系统抗风险能力。

4.3 保障业务连续

通过异构多活交易信息系统的建设，实现异构多活交易节点之间数据的准确性和一致性，在某一交易中心故障场景下，正常交易中心可以承载全部客户的交易业务，保障客户交易业务的连续性。

4.4 支持业务扩展

通过异构多活交易信息系统建设，期货公司可实现对客户的差异化管理，让不同的客户对接不同的柜台系统，满足客户个性化交易需求，扩展交易业务处理能力，提升期货公司业务承载容量与服务实体经济能力。

5 建设思路

5.1 基本原则

异构多活交易信息系统建设的基本原则如下：

- a) 确保安全：确保系统安全、可靠，业务连续稳定运行；
- b) 协同管理：结合生产主交易中心部署运行情况，整体规划、统筹协同管理；
- c) 经济可行：根据成本与风险平衡原则，在满足多活交易需求的情况下，降低建设与运营成本，建设经济适用的异构多活交易信息系统；
- d) 方案成熟：选用成熟的产品和技术方案，保证系统稳定高效运行，满足和适应期货行业创新发展的要求。

5.2 组织保障

5.2.1 组织架构

期货公司根据自身的发展战略、业务特点及信息系统运行环境，科学构建异构多活交易信息系统的组织架构，明确决策层、管理层及执行层三层职能体系，实现权责分明、协同高效、纵向贯通。各层级岗位设置覆盖建设、运维、应急、安全等关键环节，确保系统稳定运行与业务连续性保障机制有效落地。

5.2.2 组织职责

决策层由期货公司高层管理者组成，决策期货公司异构多活交易信息系统建设的重大事宜，主要职责包括：确定期货公司异构多活交易信息系统战略，审核批准期货公司异构多活交易信息系统策略、经费预算、建设方案、应急切换方案、应急响应决策以及对外情况通报和信息发布。

管理层由期货公司的业务部门、技术部门、运营部门等相关部门负责人组成，在决策层领导下开展工作，负责异构多活交易信息系统建设的前期规划、建设以及后期管理和协调，主要职责包括：组织制定异构多活交易信息系统应急策略，编制异构多活交易信息系统经费预算，负责异构多活交易信息系统规划、设计、施工、测试、试运行、交付的管理工作，负责异构多活交易信息系统运维的管理工作，组织制定异构多活交易信息系统应急预案，组织

实施异构多活交易信息系统应急预案的演练，组织和管理对外情况通报和信息发布工作，监督、检查和总结异构多活交易信息系统建设工作。

执行层由期货公司的技术部门工作人员牵头，业务部门、运营部门等相关部门工作人员配合。执行层在管理层的领导下，负责期货公司异构多活交易信息系统建设的具体实施工作，主要职责包括：提出期货公司异构多活交易信息系统建设需求和策略建议，实施期货公司异构多活交易信息系统设计、施工、测试、试运行、交付等工作，实施期货公司异构多活交易信息系统运维工作，负责应急预案的制定、测试、培训、演练和管理，实施应急响应和应急保障工作。

异构多活信息系统的运维团队与主系统运维团队完全独立，实行物理隔离、权限分控、操作分离，防止操作风险叠加。

5.3 基础设施

5.3.1 选址布局

异构多活交易信息系统选址布局应符合监管部门和交易所对交易系统的相关要求，期货公司根据成本风险平衡原则选址布局，充分对场地风险评估，考虑场地周边环境、地质地理条件、市政配套条件、电力供应条件以及通信服务商所能提供的服务能力等诸多因素，全面判断是否符合建设要求。

5.3.2 基础环境

异构多活交易信息系统配套的机柜机房等基础设施资源需满足监管部门和交易所的相关要求。

5.3.3 网络建设

异构多活交易信息系统网络建设需要满足业务连续性及重要业务指标峰值所需的带宽需求，并且需实现生产网与互联网的有效隔离管控，保障异构多活交易信息系统生产环境网络安全。期货异构多活交易系统采用跨机房多活部署架构。在单个机房内部，各业务区域之间通过二层的万兆网络进行高速数据交互；跨机房之间则依托运营商裸光纤或大带宽专线实现级联，以保障网络低时延与高可靠性。双机房在内部网络结构上保持严格一致，均设有互联网区、前置交易区、内部互联区、网络报盘区、专线接入区等，从而实现功能对等与业务无缝切换。

在跨机房数据传输方面，系统根据业务特征实施差异化策略：盘中实时交易类数据（如账户、资金及密码信息）需确保高时效与安全传输；而盘后全量账户、结算数据以及日常归档数据等非实时业务，则可在业务低峰时段调度传输，并配合持续的网络容量监控与资源保障，确保整体传输效率与系统稳定性。

5.4 系统要求

5.4.1 能力要求

异构多活交易信息系统部署模式支持并行运行，能承载期货公司全部客户的交易、结算、风控、转账等业务，支持数据的实时同步与备份，关键组件冗余部署、无单点故障，支持盘中客户快速切换，确保客户的交易、转账业务不受影响，期货公司风控、结算业务正常运行。

5.4.2 功能要求

具备对客户交易进行盘中实时风险控制的功能，支持验资验仓，产生、记录并存储必要的日志信息供审计，具备对客户交易接入认证与授权管理功能，具备客户交易密码安全管理功能，具备客户交易中心权限管理的功能，支持对客户进行交易中心切换，满足监管机构和交易所对交易信息系统的相关要求。

5.4.3 系统性能

异构多活交易信息系统的性能和容量应达到交易所对会员交易系统的所有要求，能承载期货公司全部客户的交易，订单与成交峰值吞吐率、订单处理与成交时延、日订单成交与行情处理容量、连接数容量、系统可靠性与稳定性等性能指标需满足监管部门和交易所的相关要求。

5.5 安全合规

5.5.1 系统安全

期货公司建设异构多活交易信息系统需符合行业标准和自身业务发展需要，制定异构多活交易信息系统的信息技术管理制度，设置相关岗位，保障信息系统安全运行。建立异构多活交易信息系统的安全监测机制，设立监测指标并持续监测重要信息系统的运行状况。

5.5.2 数据完整

异构多活交易信息系统的安全防护措施能够保障期货公司的经营数据和客户信息的安全、完整，需建立对异构多活交易信息系统的数据备份管理制度，妥善保管客户资料、委托记录、交易记录等数据信息。

5.5.3 功能合规

异构多活交易信息系统的功能设计与技术实现应当合规，各项功能符合法律、行政法规以及中国证监会的有关规定，期货公司运行管理能力和信息系统备份能力能够保障信息系统的权限清晰、风险可控、运行稳定。

6 建设方案

6.1 方案选型

6.1.1 全面覆盖业务场景

期货公司根据自身业务开展情况，系统梳理经纪业务、做市商、交割、质押、国际化、期转现、银期转账等业务需求，确保异构多活交易信息系统能完整支持本公司业务。

6.1.2 精准评估性能容量

期货公司根据主交易系统的历史数据，统计一定周期内的历史峰值订单吞吐速率、委托容量、成交容量、持仓容量、订单延时等数据，评估异构多活交易信息系统是否能满足本公司的性能和容量要求，并为未来业务增长预留充足余量。

6.1.3 具备高效接管能力

期货公司在方案选型时需充分考虑切换操作便捷性、耗时和风险。异构多活交易信息系统需具备完善的应急操作指引，当主交易系统发生故障时，期货公司能根据操作指引，让异构多活交易信息系统快速便捷地接管故障系统的交易业务，保障业务连续。

6.1.4 深度适配周边系统

异构多活交易信息系统需与现有周边系统实现对接，包括：各类型交易终端与中继产品、各类次席柜台系统、各类程序化接入服务、CRM、反洗钱、适当性、报表系统、资管系统、短信平台、财务系统等。应提供标准化接口文档，降低对接成本。

6.1.5 综合成本效益评估

期货公司需从硬件成本、软件成本、管理成本等多维度进行综合评估。硬件成本包括但不限于服务器、存储、网络设备等，软件成本包括但不限于数据库、中间件、监控工具等，管理成本包括但不限于运维、业务使用、培训等。

6.1.6 满足信创合规要求

异构多活交易信息系统需满足国产商用密码的安全性要求，从CPU、操作系统、数据库、系统软件等维度考虑信息技术创新应用的案例，参考“安全可靠测评”名录，选择更加安全可靠的异构多活交易信息系统方案。

6.1.7 技术方案成熟可靠

选择已在证券期货行业成功落地、有同类型生产运行案例的供应商。审阅其技术文档、测试报告、部署方案等，参考已落地客户的建议。

6.1.8 提供持续技术支持

异构多活交易信息系统供应商需建立专属服务团队，提供及时有效的技术支持，确保系统稳定运行，同时供应商需定期对系统进行迭代维护，修复漏洞并优化性能。

6.2 系统测试

6.2.1 对比测试

为保障异构多活交易信息系统与主用系统间的业务连续性和数据准确性，须依据真实的业务场景，构建数据一致性校验机制，测试覆盖核心业务数据域，包括但不限于：

- a) 客户账户信息
- b) 客户交易权限
- c) 客户资金
- d) 手续费率和保证金率
- e) 客户持仓

6.2.2 功能测试

基于异构多活架构特性，制定覆盖全业务流程的系统测试方案和标准化测试用例集，对关键模块功能进行深度验证，测试范围包括但不限于：

- a) 账户管理：开户、销户、信息变更
- b) 资金管理：入金、出金、冻结
- c) 交易业务：委托、撤单、成交、行权

- d) 风险管理：风险监控、风险预警、强平、预结算
- e) 结算管理：日终结算、持仓对账、资金对账、结算单生成

6.2.3 安全测试

异构多活交易信息系统在上线前根据实际需求，编制详细的安全测试计划和测试用例，执行相关测试并确保测试结果符合期货行业安全等级要求。测试内容包括但不限于：

- a) 安全功能检查：通过人工检查、审核的方式对软件开发过程中涉及的安全策略、技术决策（如开发模型等）进行安全功能检查；
- b) 代码安全测试：通过对软件源代码进行安全扫描和审计，排除代码中的漏洞（如外购类软件系统，可由开发商提供代码安全测试报告）；
- c) 漏洞扫描：通过扫描等手段对指定系统进行检测，发现可利用漏洞；
- d) 渗透测试：以攻击者视角进行的黑盒测试，获得对应用系统的安全评价；
- e) 模糊测试：以向目标系统提供非预期输入的方式，验证系统对意外输入的容错能力。

6.2.4 冗余测试

为确保异构多活交易信息系统的高可用性，系统架构需基于行业特点采用多活或冷备等冗余部署策略，增强容错能力与业务连续性。在投产前，应全面验证冗余机制的有效性，重点测试节点故障（如宕机、网络中断、硬件异常等）场景下备份节点的快速接管能力，确保业务连续性。通过模拟各类异常情况，严格评估系统的故障恢复时间（RTO）、数据一致性（RPO）及备节点业务承载性能，为系统稳定运行提供可靠支撑，最大限度降低单点故障对业务的影响。

6.2.5 压力测试

异构多活交易信息系统的性能测试需重点关注两类核心指标：一是容量性能指标，包括系统在高负载下的处理能力、最大吞吐量以及业务成功率；二是资源效率指标，涵盖CPU、内存、磁盘I/O和网络带宽等系统资源利用率，以及业务平均响应时间和长尾延迟。通过设计覆盖正常、峰值及故障场景的多样化测试方案，全面验证系统在高并发大流量下的稳定性，测试完成后需形成详尽的压力测试报告，为系统优化提供数据支撑，确保各项关键指标始终处于合理可控范围，有效保障系统容量与业务需求的持续匹配。

6.2.6 交易中心切换测试

为验证交易终端在多中心环境下的高可用性，需结合业务需求制定详细的交易中心切换测试方案。测试用例设计应重点覆盖以下方面：

- a) 连接正确性，确保终端能精准识别并连接目标交易中心；
- b) 数据完整性，验证切换过程中无数据丢失或异常；
- c) 切换稳定性，测试不同网络条件下的平滑切换能力；
- d) 投资者体验，评估切换过程对投资者操作的实时影响。
- e) 通过模拟中心切换、网络抖动等场景，全面验证终端程序在异常情况下的自动恢复能力，确保业务连续性和无缝切换体验。

6.3 系统上线

6.3.1 上线策略

异构多活交易信息系统上线前需根据系统部署方案，制定详尽的系统上线方案，做好完善的上线计划。上线方案可包括上线参与方、参与人员、上线时间、前序准备工作、上线详细操作步骤等。

6.3.1.1 交易系统上线

异构多活交易信息系统上线可按照实际情况采用试运行与双轨运行结合分阶段渐进方案，试运行阶段以灰度发布方式逐步开放功能，优先覆盖低风险业务，同步实施全链路监控与数据对账验证，快速迭代优化。双轨运行阶段异构多活交易信息系统与主用系统保持并行运行，重点验证交易一致性、数据完整性与系统稳定性，期间持续收集运行指标并开展性能调优。

6.3.1.2 交易终端上线

在交易终端上线过程中，可采取分阶段推进策略，按照投资者使用占比从低到高分步上线。同时要强化风险管控，梳理潜在风险点并建立分类评估机制，针对各类风险制定详细的应急预案和处置流程，确保升级过程平稳可控。

6.3.2 上线实施

6.3.2.1 上线前置条件

- a) 异构多活交易信息系统已完成全部技术准备工作，相关系统应用已全部部署；
- b) 已通过对比测试、业务功能测试、安全测试、冗余测试等多项测试，系统业务数据处理效率、承载容量及整体性能指标均符合设计要求；
- c) 交易中心切换测试工作已全面完成；
- d) 相关人员已完成系统操作规范的专业培训，人员分工及岗位职责（包括系统操作岗、技术维护岗、运营管理岗等）均已明确落实。

6.3.2.2 上线前准备

- a) 确定上线具体参与人员，做好上线实施工作及上线后的监控工作的人员安排，并根据上线情况，向领导小组进行报告；
- b) 制定上线计划，按步骤编写实施方案，方案包含不限于具体实施步骤、业务验证方案、测试用例等，并做好相关验证工作；
- c) 制定应急回退方案，包括回退工作的具体操作步骤、回退指标、后续检验步骤等。在上线前进行系统回退演练，确保方案切实可行；
- d) 异构多活交易信息系统上线前，对公司内部业务、客服等相关人员做好统一培训。

6.3.2.3 上线实施

组织参与实施人员按照上线方案的操作步骤操作，在开盘前完成切换，并调整好系统监控项。切换完成后，做好相关验证工作，使用测试账号进行基础业务测试，确保系统功能正常、数据准确无误。

6.3.2.4 上线跟踪

信息技术团队对已上线的异构多活交易信息系统进行全生命周期运维监控，实时跟踪系统运行状态、用户操作行为及投资者在线数据，并通过收集分析用户反馈持续优化系统功能，针对发现的问题及时制定并实施改进方案。

7 运行保障

7.1 业务保障

7.1.1 业务承载

进行异构多活交易信息系统的参数管理、客户迁移、权限管理等工作，确保异构交易信息系统能承载部分客户交易，委托、转账、行权等功能能正常使用。

7.1.2 并行结算

每日交易结束后，在主交易系统和异构多活交易信息系统上分别进行结算，结算流程包括：

- a) 数据准备：导入交易所结算文件，完成数据同步。
- b) 业务处理：包含资金处理、交割处理等盘后业务。
- c) 清算处理：计算保证金、盈亏、手续费等。
- d) 数据核对：交易所结算数据核对。
- e) 报表生成：生成结算报表，如成交明细、资金流水等。
- f) 合规报送：向监控中心报送看穿式采集信息与结算数据。

7.1.3 数据稽核

在结算后，需确保两套系统的数据一致性，包括账户数据、交易数据、持仓数据、资金数据等。

稽核时间：每日结算完成后，立即进行数据稽核。

稽核内容：对比两套系统的核心数据，确保数据匹配，例如：

- a) 交易数据：包括成交价格、数量、时间、方向等。
- b) 持仓数据：包括合约代码、持仓量、方向等。
- c) 资金数据：包括账户余额、可用资金、冻结资金等。

稽核方法：

- d) 自动稽核：开发数据比对工具，自动对比两套系统的数据，并生成差异报告。
- e) 人工稽核：对自动稽核发现的差异进行人工核查，分析原因并解决问题。

差异处理：

对于数据不一致的情况，需及时查明原因并进行处理。

如果差异是由于异构多活交易信息系统数据延迟造成的，需等待数据同步完成后再进行稽核。

如果差异是由于其他原因造成的，需及时修复问题并重新进行结算和稽核。

7.1.4 数据同步

为减少手工操作，提升运营效率，降低业务风险，需实现主备和异构系统间数据同步，按同步时间要求分为实时同步和非实时同步，需实时同步的数据有：账户信息、交易编码、资金、交易密码、资金密码、交易权限、银期签约数据。非实时同步的数据有：客户基本信息、出入金数据、分项资金、交易权限数据、产品合约信息、现货行情信息、组织机构信息、交易所保证金率、公司标准保证金率、客户保证金率、交易所手续费率、公司标准手续费率、客户手续费率、申报费率、仓单质押信息、交割信息、看穿式采集信息。

7.2 技术保障

7.2.1 监控范围

基础设施层

服务器: CPU 使用率、内存使用率、磁盘空间、硬件状态等。

网络设备: 网络延迟、丢包率、带宽利用率、设备状态等。

存储设备: 存储空间使用率、读写性能、设备状态等。

软件层

操作系统: 系统负载、进程状态、文件描述符使用情况等。

中间件: 连接数、线程数、队列长度、响应时间等。

数据库: 连接数、SQL 执行时间、锁等待时间、缓存命中率等。

应用软件: 交易接口响应时间、订单处理速度、风控处理效率、数据同步效率等。

业务层

应用日志: 错误日志、警告日志、关键操作日志等。

7.2.2 监控指标

性能指标: 反映系统运行效率和资源使用情况, 例如响应时间、吞吐量、并发数、数据同步堆积等。

可用性指标: 反映系统可用性和稳定性, 例如进程运行状态、组件连接状态、服务可用率、故障恢复级别和时间等。

容量指标: 反映系统资源使用情况和容量瓶颈, 例如 CPU 使用率、内存使用率、磁盘空间、带宽利用率等。

业务指标: 反映系统业务运行状况, 例如订单成交率、撤单率、风险事件发生率等。

安全指标: 反映系统安全状况, 例如登录失败次数、敏感操作记录等。

7.2.3 报警机制

报警时机: 当出现影响系统正常运行的软硬件错误或性能风险时, 触发报警。

报警方式: 提供合适的报警方式, 例如监控平台提示、邮件、短信、微信、电话等。

报警级别: 根据指标的重要性和紧急程度设置不同的报警级别, 例如警告、严重、致命等。

报警处理: 建立完善的报警处理流程, 确保报警能够及时得到处理。

7.2.4 容量管理

异构交易信息系统须建立全生命周期、动态可预测、量化可评估的容量管理体系, 确保系统在业务高峰、市场波动、极端行情等压力场景下仍能稳定运行, 满足监管机构对会员系统性能的持续性要求。建立基于历史交易数据、客户增长趋势、未来三年容量预测模型, 覆盖订单处理峰值吞吐率(笔/秒)、同时在线连接数、日均成交单量、数据存储增长速率进行容量规划, 每季度开展容量健康度评估, 设定冗余阈值, 预留弹性扩容空间应对突发流量。

7.2.5 补丁管理

为保障异构交易信息系统安全、稳定、合规运行, 须建立标准化、可追溯、风险可控的补丁管理机制, 统筹软件漏洞修复、安全增强与版本升级, 杜绝因补丁管理缺失引发的系统性风险。补丁管理流程如下:

a) 识别评估: 根据交易所通告、厂商公告, 评估影响范围与业务影响;

- b) 测试验证：在独立测试环境进行功能、性能、兼容性、切换能力测试，形成《补丁测试报告》；
- c) 审批排期：由管理层组织技术、运维、合规三方联合评审，确定上线窗口，纳入变更管理工单；
- d) 灰度发布：优先在备用节点部署，观察一段时间确认无异常后，按预案同步至主备系统；
- e) 补丁回滚：如遇异常，启动回滚方案。

7.3 应急方案

7.3.1 应急准备

期货公司成立应急工作领导小组，负责公司应急工作的组织、协调和指导。

a) 应急工作领导小组的职责：

组织制定和修订应急管理制度；

组织编制和修订应急预案；

组织开展应急演练；

负责应急物资、应急设备的采购、管理、维护。

b) 应急处置联络手册内容

分层分级管理：建立决策层、技术负责人、操作层三级联络体系，覆盖交易所、结算银行、外部技术供应商、监管机构等关键方；

动态更新机制：每月核查一次通讯录，重大系统变更后 24 小时内更新，并同步至企业即时通讯软件及邮件组；

合规报备清单：明确需向监管机构报告的故障类型（如全市场中断超过 5 分钟）、报送时限（如 30 分钟内）及渠道（证监会应急管理平台）。

c) 应急预案及演练操作

场景库建设：覆盖《证券期货业信息系统应急管理指南》中 I-IV 级事件，重点设计以下场景：

主备数据中心网络出现重大故障；

异构多活交易信息系统间订单流不一致导致资金风险敞口；

交易所 API 异常引发的报单阻塞；

开展无脚本演练，模拟开盘前 30 分钟主席系统核心组件崩溃，考核异构多活交易信息系统接管时效（目标 RTO≤3 分钟）；

演练评估指标：记录故障发现时间（MTTI）、决策时间（MTTD）、恢复时间（MTTR），要求年度演练覆盖率 100%。

7.3.2 应急处置

a) 应急响应流程

事件定级列表如表1所示。

表1 事件定级列表

等级	判定标准（示例）	响应要求
I 级	全市场交易中中断≥10 分钟	15 分钟内启动灾难恢复，向证监会提交书面报告。

表1 事件定级列表（续）

等级	判定标准（示例）	响应要求
Ⅱ 级	单个系统故障影响≥20% 客户	30 分钟内切换至异构多活交易信息系统。

熔断机制：当检测到主席系统报单成功率低于 95% 持续 1 分钟，自动触发交易流量切换至异构多活交易信息系统；

资金安全兜底：切换期间启用风控系统的资金试算功能，确保客户保证金覆盖率≥100%。

b) 监管协同

向各期货交易所同步报送系统状态，报备紧急平仓；

关闭银期转账功能，防止切换期间的重复出金。

7.3.3 典型应急场景

典型应急场景列表如表2所示。

表2 典型应急场景列表

场景	处置要点
主席与异构多活交易信息系统订单簿差异超过 0.1%	a) 暂停新订单录入 b) 启动差异订单比对工具（基于 Timestamp 和 OrderID） c) 以主席系统为基准执行数据修复
异构多活交易信息系统内存泄漏导致响应延迟≥500ms	a) 隔离故障节点并转交开发团队分析 b) 启用轻量化应急交易通道（仅支持限价单）
银期转账对账不平（T+0 18:00 前未修复）	a) 调用银行系统冲正接口撤销异常流水 b) 通过人工指令完成日终结算资金调拨
主系统宕机且无法自动恢复	a) 故障检测 b) 无缝切换，API网关将客户批量迁移至异构多活交易信息系统 c) 特殊处理，如对故障时的订单状态处理
主用系统与异构多活交易信息系统生成的结算文件存在差异	a) 比对关键字段信息差异 b) 确定差异原因 c) 解决故障系统问题 d) 使用正确结算文件报送
信创环境因芯片或OS级缺陷导致崩溃	a) 切断信创系统交易链路 b) 切换至异构多活交易信息系统

7.3.4 主席系统故障应急方案

主席系统故障应急方案列表如表3所示。

表3 主席系统故障应急方案列表

场景	应急方案	处置要点
主席交易故障	a) 通过 F5 负载均衡器将交易 IP 切换至异构多活交易信息系统 b) 校验未成交订单状态(撤单重发或保留原订单号) c) 监控异构多活交易信息系统每秒订单吞吐量	确保切换过程中交易连续性,避免订单丢失。
主席风控故障	a) 启用异构多活交易信息系统的实时风险试算模块 b) 动态调整保证金计算规则	实时监控风险指标,确保风控措施有效。
主席银期故障	a) 切换银期网络至异构多活交易信息系统的银期组件环境 b) 启用异构多活交易信息系统的冲正机制,自动修复单边账	确保银期数据一致性,避免资金有误。
主席结算故障	a) 切换至异构多活交易信息系统的结算子模块 b) 调用交易所 API 重新下载 T 日结算数据	确保结算数据准确,避免结算错误。
主席账户故障	a) 启用备份账户系统 b) 修复账户数据 c) 数据一致性检查	检查账户状态,确保账户信息完整。

7.3.5 异构多活交易信息系统故障应急方案

异构多活交易信息系统故障应急方案列表如表4所示。

表4 异构多活交易信息系统故障应急方案列表

场景	应急方案	处置要点
异构柜台交易故障	a) 灰度切回:按客户号段分批迁移(如先切换机构客户) b) 确保主席系统订单流水号连续,避免交易所拒单	确保切回过程中交易连续性,避免订单丢失。
异构柜台银期故障	补发异构多活交易信息系统切换期间的出入金流水	确保银期数据一致。
异构柜台结算故障	修复异构多活交易信息系统的持仓数据差异(以交易所为准)	确保结算数据一致。

附 录 A

(资 料 性)

案例1：全业务异构多活建设方案

A.1 方案概述

本案例为包括交易、银期、风控、账户、结算的全业务异构多活建设方案。异构多活系统的架构可以分为主系统、异构系统、系统间数据同步链路。目标是异构系统可以独立承接公司日常交易、结算业务，主系统与异构系统数据保持一致，客户盘中切换交易中心后仍能正常交易。

异构系统交易模块部署独立的交易所席位，直连交易所，盘中接收全量客户回报，保证客户资金、持仓与主系统相同，客户盘中密码修改、出入金请求，转发至主系统处理，保证应急切换时客户密码、资金、持仓数据一致。在交易前置和终端之间设有中继网关层，中继网关层配置客户的交易通道路由，负责将客户的请求转发至主系统或异构系统。

异构系统风控模块不对接外部系统，数据依赖交易模块，可承担全量客户的风险监控。

异构系统银期模块分为有报盘模式和无报盘模式。有报盘模式的部署，需要在异构系统、主系统与银行中间部署银期统一管理平台，负责将多活系统的银期请求统一转发至银行。无报盘模式的部署，需要额外部署银期请求转发组件和资金同步工具，将异构系统的银期请求转发至主系统处理，由主系统统一上报银行，异构对主系统的回报进行处理。主系统的出入金通过资金同步工具实时同步至异构系统，保证异构多活系统之间的资金一致性。

异构系统结算模块独立部署，费率等数据可通过盘后同步组件从主系统同步至异构系统。日常独立结算，结算后与主系统进行对账，确保结算数据一致。

异构系统账户模块不对接监控中心，日常账户业务在主系统办理，异构系统通过系统间数据同步链路实现全量客户信息或增量客户信息同步。

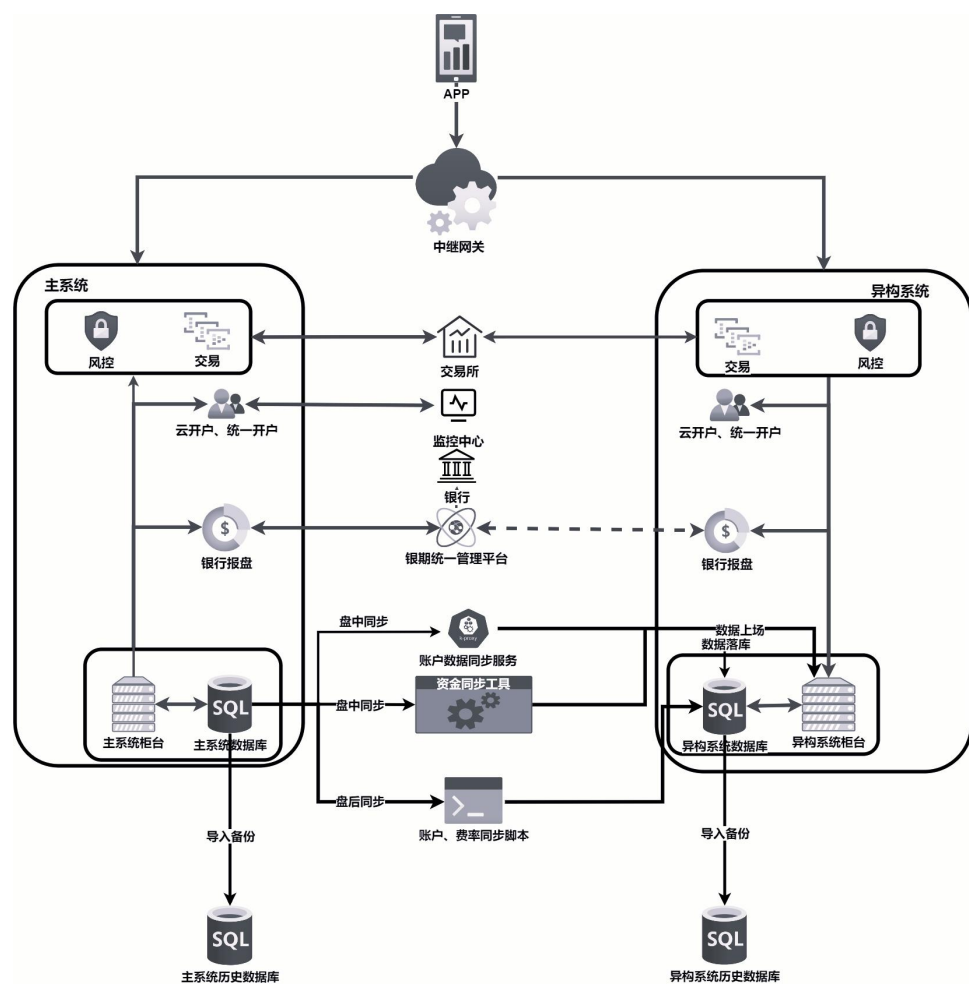


图 1 异构多活系统架构图

A.2 交易多活方案

A.2.1 交易多活原理

a) 多活密码同步原理

主系统与异构系统密码一致，是多活系统交易模块盘中并行的一项基本要求，可以保证盘中客户切换交易中心时仍能继续交易。

客户在主系统修改密码，可通过盘中同步链路将新密码同步至异构系统，异构系统支持主系统的密码加密方式，保证客户使用相同密码可在异构系统登录。

客户在异构系统修改密码，可通过异构柜台使用中继操作员模式向主系统发起接口调用，在主系统完成客户密码修改，修改后的密码再通过盘中同步链路同步至异构系统。

b) 多活手动切换原理

目前主流的交易多活设计模式核心为在终端与异构多活系统之间增加中继网关层，中继网关层会配置客户与交易中心的路由关系表。客户使用终端发出请求后，请求首先会发送至中继网关层，中继网关对请求进行处理后，根据配置好的路由关系，调用客户所在柜台的 API，将请求发送至柜台，柜台处理请求后，将回报数据转发返回给终端。如果投资者因业务需要，需要由主系统切换至异构系统，一般选择收市之后进行切换，根据切换需求，设置

此类账号的登录系统策略，同时修改投资者在路由关系表，再次登录即可进入切换后系统，该切换对于投资者是无感知的。

c) 多活批量切换原理

如果主系统因系统故障无法交易，需要把主系统所有投资者切换至异构系统进行交易，先在中继网关层将投资者在所属交易中心批量修改为异构系统，再使用一键切换功能，投资者和主席柜台连接被断开，投资者重新登录后则已切换至异构系统。

A.2.2 交易切换流程

当主用交易系统发生故障时，需将客户切换至异构系统以保障业务连续性，切换方案如下：

- a) 调整中继网关层客户交易中心的路由关系，使用一键切换功能，所有客户切换登录至异构系统；
- b) 关闭主用系统前置服务；
- c) 关闭主用交易系统至异构系统的数据同步服务；
- d) 登录异构系统，监控客户登录情况；

A.3 风控多活方案

异构系统风控模块部署方式与主系统风控模块相同。

A.4 银期多活方案

A.4.1 银期多活原理

期货公司的银期多活技术发展出两种模式：一是无报盘的异构系统模式，二是具备报盘功能的多活模式，以兼顾接入规范与系统高可用性需求。

a) 无报盘模式

异构系统在收到客户银期请求后，会将其转发至主交易系统进行处理，待主系统接收到银行回报并处理完毕，通过资金同步工具将最终结果实时同步至异构多活系统。

b) 报盘模式

银期统一接入网关在银行与交易系统之间构建了统一的中间层，实现了银期的多活运行。交易系统不直接与银行进行业务交互，而是通过银期网关将业务消息转发至银行。银行端发起的银期请求统一由主银期系统处理，并将结果同步至其他交易系统。期货端发起的银期请求由主用交易系统和异构系统进行处理，成功后将请求发送至银期统一接入网关。网关作为统一枢纽将请求转发至银行，并在收到银行应答后，依据流水号将结果精准返回至原始发起请求的交易系统，并将结果同步至其他交易系统。

A.4.2 银期模块部署方式

a) 无报盘模式部署

异构系统不部署银期报盘，只有主交易系统部署银期报盘对接银行，异构系统出入金业务转发至主系统处理，异构系统针对主系统处理结果进行处理。

b) 报盘模式部署

异构系统部署银期报盘，银期报盘不与银行直接对接。主系统和异构系统同时对接银期统一接入网关，银期统一接入网关对接银行，将银行的回报同时发给主系统和异构系统。

A.4.3 银期切换方案

部署有银期统一网关的异构多活系统，单系统银期故障时，不会影响其他多活系统。

a) 主用系统银期故障

修改银期统一接入网关设置，将异构系统为主银期系统。关闭主系统银期模块组件。

可以通过调整中继网关层客户和交易中心的路由关系，将客户切换登录至异构系统，已登录主系统的客户会有掉线情况，但重新登录后恢复正常。也可以让客户继续留在主系统交易，但只能通过银行端办理银期业务。

b) 异构系统银期故障

将异构系统银期模式调整为无报盘模式，异构系统银期请求全部转发至主系统进行处理。

A.5 结算多活方案

A.5.1 结算模块部署方式

异构系统结算模块部署方式与主系统结算模块相同。

A.5.2 结算流程

在结算流程中，使用数据同步脚本，从主系统同步费率、交割、质押等数据到异构系统，降低运营人员维护多套系统成本。异构系统结算后使用数据库脚本方式与主系统进行资金持仓对账。

A.6 账户多活方案

账户业务办理系统通常选用主系统，异构系统不直接对接监控中心进行业务办理，账户数据从主系统实时同步或盘后批量同步。账户模块仅需部署账户数据查询服务，供业务人员查询使用。

附录 B

(资料性)

案例2：核心模块异构多活建设方案

B.1 方案概述

本案例为交易、风控核心模块异构多活建设方案。通过最小化的基础设施投入，部署轻量化异构多活系统，实现系统高可用性和业务连续性保障，为核心交易系统构筑起最后一道安全防线。异构交易中心日常处于“不活跃”状态，禁止客户登录，仅提供交易员应急下单通道；紧急情况下交易中心切换为启用状态，允许客户登录和交易，降低日常运维成本和系统风险。

轻量化异构多活系统采用交易模块建设模式，交易系统架构包括前置集群、报盘集群、交易核心集群、管理服务、数据同步服务。

前置集群负责提供客户端及中继网关的接入服务；报盘集群负责六所报盘接入；交易核心集群负责交易业务处理，确保各项业务逻辑与主席柜台一致；管理服务提供异构系统的内部操作管理；数据同步服务主要提供系统内部数据的上下场功能。

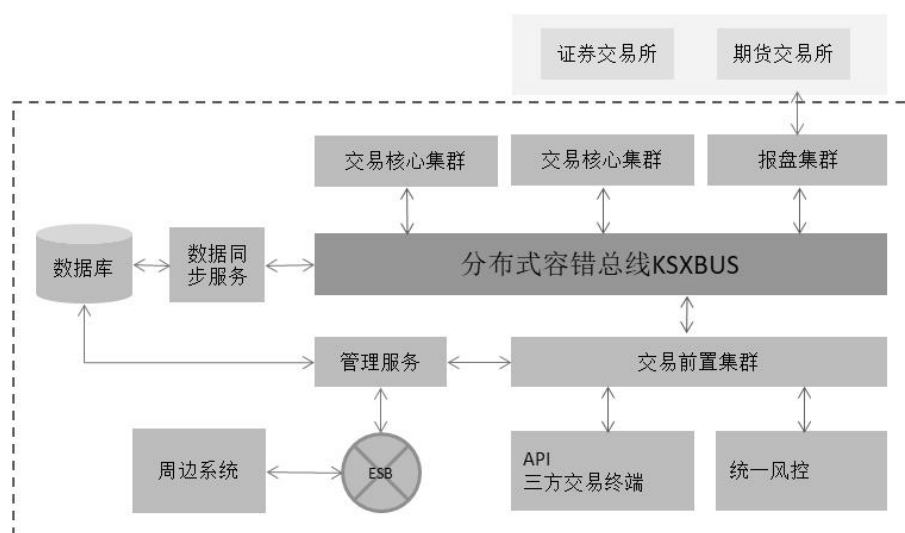


图 2 交易系统架构图

异构交易系统作为主柜台系统的备份和应急系统，在主柜台系统出现交易故障时能够快速接管业务，与主席系统的业务逻辑图如下：



图3 异构灾备业务逻辑图

每日结算完成后,通过主席系统分发结算文件给到异构系统系统进行下一交易日数据的准备及日切;异构系统在盘中交易时通过同步工具同步主席的出入金数据来保证金客户资金与主席系统的一致性。

B.2 交易多活方案

交易模块的部署主要包含前置区、核心区、报盘区,前置区包括交易前置、行情前置等组件,核心区包括交易核心、总线、仲裁等组件,报盘区包括交易报盘、行情报盘等组件。客户通过前置区接入系统,发送报单请求,报单请求经过总线对订单定序后,转发至交易核心处理,再转发至报盘区,最终由报盘区将订单发往交易所。

B.3 风控多活方案

异构风控部署提供两种方案:方案一为部署依赖异构交易系统的风控模块;方案二为部署独立的异构风控系统。

B.3.1 异构系统集成风控模块

部署依赖异构交易系统的风控模块,风控模块接收交易系统推送的委托、成交、行情等数据,处理投资者的各项风险预警与指标监控,并提供试算和风险通知等功能。

B.3.2 独立异构风控系统

搭建独立的异构风控系统,配置专用的交易所报盘,直接从交易所收取委托回报、成交回报和行情信息,从期货主系统同步出入金流水,日初同步主系统结算数据,确保与生产主系统的数据一致性。

集成风控模块和独立风控系统方案对比如表5所示。

表5 集成风控模块和独立风控系统方案对比

对比项	集成风控模块	独立风控系统
优势	a) 节省席位资源 b) 系统部署简便 c) 日常运维便利	a) 不依赖交易系统运行 b) 功能扩展性更强
劣势	依赖交易系统正常运行	a) 增加席位资源投入 b) 运维复杂度提升

参 考 文 献

[1] 《期货公司监督管理办法（证监会令〔第155号〕）》2019年6月4日由中国证券监督管理委员会发布，自2019年6月4日起施行

[2] 《证券期货业网络和信息安全管理暂行办法（证监会令〔第218号〕）》2023年2月27日由中国证券监督管理委员会发布，自2023年5月1日起施行
