ICS 35.240.40
CCS A 11

JR

# 中华人民共和国金融行业标准

JR/T 0209—2021

# 金融信息系统多活技术规范 应用策略

Multi-active technology specification of financial information system—

Application strategy

2021－02－07 发布　　2021－02－07 实施

中国人民银行　发布

# 目　　次

# 前　言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》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。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国人民银行科技司、网联清算有限公司、中国人民银行清算总中心、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、财付通支付科技有限公司、支付宝（中国）网络技术有限公司、北京度小满支付科技有限公司、网银在线（北京）科技有限公司、中国平安保险（集团）股份有限公司、交通银行股份有限公司、中国邮政储蓄银行、招商银行股份有限公司、上海浦东发展银行股份有限公司、中信银行股份有限公司、中国民生银行股份有限公司。

本文件主要起草人：李伟、陈立吾、罗永忠、贺铁林、周祥昆、宁翔、强群力、詹志建、刘帅、刘永钢、李耘平、郭林、闵远利、金增、浦沅、范建晓、杨凌、陈晨、谢磊涛、党文轩、谢进、胡长晰、来翔、李兵、崔永刚、陈俊、薛松源、马梯恩、倪运伟、孔楠、赖海龙、李雾伦、周祥为、马兵、孙宇鹏、刘元勋、张宸铭。

# 引　言

金融业关系国计民生，维护金融信息系统安全是国家信息安全的重点，因发生灾难导致金融服务中断，可能对企业内部管理、公民、法人和其他组织的金融权益甚至国家金融稳定和秩序产生影响，在以往的标准中，对金融信息系统的灾难恢复和业务连续性进行了规范,但未涉及多活技术的规范。

为规范和引导在金融信息系统合理运用多活技术实现业务承载和灾难恢复,有效防范金融信息系统风险，保护金融机构客户的合法权益，特编制本文件。

# 金融信息系统多活技术规范 应用策略

## 1 范围

本文件规定了金融信息系统多活技术的应用场景、应用策略、演进路线。

本文件适用于金融领域信息系统的规划、设计、建设和维护。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0207—2021 金融信息系统多活技术规范 术语

JR/T 0208—2021 金融信息系统多活技术规范 参考架构

## 3 术语和定义

JR/T 0207—2021界定的术语和定义适用于本文件。

## 4 概述

本文件提出了金融信息系统多活技术的应用指南，金融机构可根据自身业务需要，结合本文件进行多活信息系统的规划、设计、建设和维护。结合多活技术的特性和金融信息系统的功能，将信息系统的应用场景分为流水型系统、账户型系统、计算型系统和查询型系统。对于不同应用场景多活技术的应用效果和应用策略存在差异。应用多活技术还应考虑充分利用现有系统资源，尽量减少改造过程中的业务影响，保障业务连续性。因此，本文件提出了金融信息系统向多活信息系统演进的策略，见附录。

## 5 多活应用场景

### 5.1 流水型系统

流水型系统实现实时支付、证券交易、订单等业务的发起方和接收方之间的转接功能，典型的流水型系统是银行渠道系统、转接清算系统、非银行支付机构的快捷支付（协议支付）系统等。对于此类系统，业务请求和业务请求响应需要实时转发至业务发起方和业务接收方，对系统的实时性有较高的要求，但关键数据（如交易涉及的账户数据）的一致性由业务发起方和接收方保证，流水型系统对业务的流水信息进行记录。

流水型系统的幂等性处理是架构设计的重点和难点，可采用多层幂等保障机制，如用户发起业务流量环节幂等、实时业务处理环节幂等、交易对账环节幂等。

采用多活技术的流水型系统，可实现业务流水信息（如订单信息、交易信息等）的多点存储和业务的多点转接，各多活子信息系统可分担流量，并且在部分多活子信息系统发生灾难或故障时，其他多活

子信息系统仍可接管业务流水信息记录和业务转接。对于处于重要业务处理路径上的流水型系统，采用多活技术可避免因流水型系统的灾难或故障造成重要业务的全业务流程中断。

### 5.2 账户型系统

账户型系统主要实现账户信息、用户信息等业务数据的处理和记录。此类系统需要优先保障关键数据的一致性，当灾难或故障发生时，应在达到关键数据一致性的前提下，实现业务可用性。

账户型系统的数据一致性是架构设计的重点和难点，应结合业务模型选择解决方案，如关键数据采用同步复制等手段、将只读数据和可写数据分离、业务处理层与数据存储层协调工作等。

采用多活技术的账户型系统，可根据需要设计各多活子信息系统的并行策略，将账户拆分到多个多活子信息系统，并行进行账务处理。当故障或灾难事件发生时，只有部分账户受到影响，并将其业务流量变更至其他多活子信息系统。

### 5.3 计算型系统

计算型系统实现清分清算、风险控制、商户结算等相关的计算，还包括金融领域的各种科学、工程、数据分析、音视频处理等相关的计算。此类系统对输入的业务进行计算，并将结果输出至其他系统，计算过程所需数据全部来源于单次计算业务请求或外部系统。此类系统重点保障计算应用的可用性和准确性。

采用多活技术的计算型系统，可实现多点计算、多点输出结果。这样可将多个子信息系统的输出结果相互核对，提高准确性，还可在部分多活子信息系统出现灾难或故障时，直接取用其余多活子信息系统的计算结果。在一些场景下，计算所需数据可能分散在分布式系统中，可能会采用多层级计算再汇总计算的方式。

### 5.4 查询型系统

查询型系统实现对用户提供各种用户信息、交易记录、交易行情、订单记录、发布信息等相关查询。此类系统中的查询应用不会对系统存储的数据进行修改（或者查询业务流量比率远远大于有数据写入和修改的业务流量的系统），数据主要由外部系统导入。此类系统重点保障查询应用的可用性，以及被查询数据的多副本存储、被查询数据的多副本之间的一致性，以保证各多活子系统查询结果相同。

采用多活技术的查询型系统，可实现多点查询。多个子信息系统之间可分担查询流量，并且在部分多活子信息系统出现灾难或故障时，可通过其他多活子信息系统查询信息。

## 6 流水型系统应用策略

### 6.1 业务模型说明

以非银行支付机构快捷支付系统为例说明多活技术在流水型系统的应用。假设该系统依赖的业务模型如下：

——需要生成并存储业务的流水记录。

——对新增业务流量的处理不依赖存量业务的流水记录，其依赖的数据均为准静态或者实时性要求不高的数据。

### 6.2 系统并行策略

流水型系统的并行策略如下：

——流水型系统可依据一定的标识进行拆分，由不同的多活子信息系统并行处理。

——拆分依据的标识可是业务流水号、用户标识信息等，还可根据需要启用用于容灾、弹性扩容等

的标识。

### 6.3 接入和路由策略

接入和路由策略包括：

——宜协同考虑参与方信息系统接入策略和多活信息系统并行策略，但接入策略可不完全依赖于并行策略。

——当业务流量发送至多活信息系统的业务接入层后，应支持根据当前各多活子信息系统的负载分布情况，选择处理业务流量的多活子信息系统。

——各多活子信息系统的业务接入层可从一定的标识中提取参与者写入的多活子信息系统的信息，将业务转发至相应的多活子信息系统处理。

——当某个多活子信息系统的处理能力不足或故障时，其业务接入层应将业务流量依次转发至其他的多活子信息系统（如可根据策略依次转到同城多活子信息系统和异地多活子信息系统）。

——对于采用互联网接入的，可引入别名机制（如 DNS 或其他类似的名字服务机制），通过别名获取接入网络地址和端口等信息。

### 6.4 数据冗余和一致性策略

数据冗余和一致性策略包括：

——业务流水应记录多副本存储，在进行业务处理的多活子信息系统存储记录主数据，在其他多活子信息系统存储副本。

——主数据与同城多活子信息系统和异地多活子信息系统的副本之间宜采用同步或异步复制机制，保证数据一致性。

——当灾难和故障发生时，应优先保障对新发起业务流量的处理时效，只需要在一定时效内达到数据一致性（即数据最终一致性）。

### 6.5 业务幂等处理策略

业务幂等处理策略包括：

——应实现多活子信息系统间的幂等，如引入全局的交易幂等记录器，全局记录业务流水号和对其进行处理的多活子信息系统的映射，用于保障多活子信息系统之间的业务幂等处理和后续查询。

——应实现多活子信息系统内部的幂等，如各多活子信息系统记录业务流水号与数据库资源的映射关系，用于保障单个多活子信息系统内的业务幂等处理和后续查询。

——可根据业务需求，采用业务最终幂等机制，允许业务在一定场景或时间内重复，后续发起反向回退机制，在幂等记录器出现故障时，应具备机制优先保证业务流量的处理和业务流水的记录。

### 6.6 可用性策略

多活子信息系统内部的可用性策略包括：

——用于存储流水记录的数据库应采用高可用架构（如分库存储等），以降低单个数据库故障的影响。

- 当某一数据库故障，将其从可用数据库资源中移除；当故障恢复后，将其加入到可用数据库资源；
- 对于每笔业务流水，从可用的数据库资源中选择数据库进行存储，通过一定策略（如轮询、随机等）均匀使用可用的数据库资源；
- 流水记录与数据库资源的映射关系模块应采用高可用架构。

——应在每个多活子信息系统内实现应用服务的高可用特性，包括但不限于实现服务注册、服务使用、服务提供的高可用。

多活子信息系统之间的可用性策略包括：

——各多活子信息系统的接入层应实现跨多活子信息系统的路由，保障在某多活子信息系统的业务处理层故障时，可将业务流量转接至其他多活子信息系统处理。

——每个参与者应同时接入多个多活子信息系统，保障在某多活子信息系统发生灾难事件时，参与者可将业务流量发送至其他多活子信息系统处理。

其他可用性策略包括：

——应符合 JR/T 0208—2021 中 7.6 的监控功能要求。

——应具备机制保证不因业务流量过大而造成多活信息系统或部分多活子信息系统的整体不可用，如限流和服务降级等机制。

——应支持配合其他业务手段（如及时发布公告等），以降低用户对故障的感知。

## 7 账户型系统应用策略

### 7.1 业务模型说明

账户型系统可能包含了流水型系统的功能，流水记录功能可能作为账户型系统的模块。账户型系统中的流水记录功能模块可参照第6章中的应用策略实现多活。

### 7.2 系统并行策略

系统并行策略包括：

——可根据账户维度进行拆分，每个多活子信息系统承载部分账户。

——应适当增加多活子信息系统的数量，以减少单个灾难事件影响的账户范围。

——对于热点账户，可采用将其拆分成多个子账户的策略，并可根据业务需求拆分为多个账户层级。

### 7.3 接入和路由策略

接入和路由策略包括：

——参与方信息系统宜依据系统拆分策略接入多活子信息系统。

——应与账户相关的流水记录模块（或流水型系统）的接入和路由功能协调考虑。

——当账户型系统发生切换时，应保证其与流水记录之间仍能正确路由。

### 7.4 数据冗余和一致性策略

数据冗余和一致性策略包括：

——账户相关数据应多副本存储，多个副本位于多个多活子信息系统。

——同城多活子信息系统的副本之间宜采用同步复制机制，保证数据强一致性。

——异地多活子信息系统的副本之间的数据一致性保证策略包括：

- 宜采用同步或异步复制机制，保证副本之间的数据一致性；
- 宜采用中间节点存储数据的方式，保证主数据与中间节点数据的数据一致性，以避免主数据与异地多活子信息系统的副本之间采用同步复制造成的时延过高；中间节点的位置选择应充分考虑灾备因素；
- 除使用多个数据副本以外，宜配合使用其他数据存储方式（例如分布式缓存、文件、日志等）对数据进行记录；可根据业务需求和其他数据存储方式的可用性启用或关闭其他数据存储方式；其他数据存储方式的存储位置选择应充分考虑灾备因素，如地理位置信息等。

——当启用备用数据时：

- 应支持实时和批量核查机制核查备用数据，应限制未核查完成的账户提供服务；
- 在核查完成但出现备用数据不一致时，可根据业务需求针对部分不依赖本地账户数据的场景继续提供服务（如入金、充值等）；
- 应支持流水记录与账户变更的核对机制。

——应考虑主数据恢复后，备份数据回切或合并的问题，避免出现多个数据副本同时提供读写，回切或合并时应隔离存在问题的数据。

——可采用保证数据最终一致性的方案解决交易数据与账户数据一致性问题，但账户数据变更未完成前，应禁止数据的再次变更。

——对于时效性有高要求的业务，可考虑配合使用应用程序和数据库的数据复制机制。

——对于采用拆分成子账户策略的系统，应分别考虑各子账户的数据一致性。

——对于热点账户，且非扣额型交易可采用延时入账的方式，即账户余额增加操作时先记录流水。

### 7.5 业务幂等处理策略

业务幂等处理策略包括：

——账户型系统的业务幂等应与相关的流水记录模块（或流水型系统）的业务幂等处理协同考虑，账户型系统宜具备自身的幂等处理模块，以避免异常情况下（如流水记录幂等失效或发生切换时）可能引起的重复账务处理。

——应通过核对流水记录等方式，规避在多活子信息系统切换过程中可能产生的重复账务处理。

### 7.6 可用性策略

可用性策略包括：

——应符合 JR/T 0208—2021 中 7.6 的监控功能要求。

——账户型系统中的流水记录模块的可用性策略可参考第 7 章实现。

——应具备机制保证不因业务流量过大而造成多活信息系统或部分多活子信息系统的整体不可用，如限流和服务降级等机制。

——应支持配合其他业务手段（如及时发布公告等），以降低用户对故障的感知。

## 8 计算型系统应用策略

### 8.1 业务模型说明

以清分系统为例说明多活技术在计算型系统的应用。清分系统采集交易记录，将交易记录汇总并按清算行维度计算借贷净额，按系统预设的时间汇总轧差，将轧差结果形成清算指令提交给清算系统。

假设清算分系统依赖的业务模型包括：

——每条交易记录具有多个副本。

——交易记录的主数据分散存储在交易系统的多个多活子信息系统中，交易系统的每个多活子信息系统有部分交易的主数据。

——交易记录的多个副本分散在交易系统的多个多活子信息系统中，交易系统的每个多活子信息系统有部分交易的副本数据。

### 8.2 系统并行策略

清分系统的输入数据是交易记录，所以清分系统各子信息系统的并行策略也依赖于输入数据，系统并行策略包括：

——各个多活子信息系统应从本地的交易系统的多活子信息系统中获取部分的交易记录。

——各个多活子信息系统应基于本地的交易记录计算清分结果。

——各个多活子信息系统的清分结果可按一定策略合并后形成全局清分结果。

### 8.3 接入和路由策略

对于清分系统，接入和路由主要解决将交易记录输入到清分系统，应考虑清分系统如何读取交易记录所在的数据源。

### 8.4 数据冗余和一致性策略

数据冗余和一致性策略包括：

——应基于交易记录的主数据和交易记录的副本数据分别计算清分结果，并对清分结果进行核对。

——可将核对一致的清分结果参与汇总，形成全局清分结果。

### 8.5 业务幂等处理策略

计算过程应以交易流水号和交易记录的数据类型（即主数据、同城备份数据、异地备份数据等）进行幂等，保证同一交易不会被重复计算。

### 8.6 可用性策略

可用性策略包括：

——应符合 JR/T 0208—2021 中 7.6 的监控功能要求。

——针对核对不一致、交易记录的主数据丢失、交易记录的副本数据丢失等情况，应分别设置判决机制，以及人工介入的兜底机制，以保证不因局部的数据不一致造成无法形成全局的清分结果。

## 9 查询型系统应用策略

### 9.1 业务模型说明

以网络支付业务的商户信息系统为例说明多活技术在查询型系统中的应用。商户信息系统提供商户的注册、信息的维护以及信息的查询。

### 9.2 系统并行策略

可在各多活子信息系统均保存全量数据，如果数据量较大，也可按某个维度拆分数据，每个多活子信息系统保存部分数据，此时用户流量分配需要和数据分布一致。

### 9.3 数据冗余和一致性策略

数据冗余和一致性策略包括：

——待查询的数据应多副本存储，多个副本位于多个多活子信息系统。

——如待查询的数据均为静态数据（如历史数据），则不必关注数据一致性的问题。

——如查询系统的数据为动态更新的数据，应关注外部数据源与查询系统数据的数据一致性。

——根据查询数据的实时性要求，数据一致性可采用强一致性或最终一致性。

### 9.4 可用性策略

可用性策略包括：

——应符合 JR/T 0208—2021 中 7.6 的监控功能要求。

——应具备机制保证不因业务流量过大而造成多活信息系统或部分多活子信息系统的整体不可用，如限流和服务降级等机制。

——应支持配合其他业务手段（如及时发布公告等），以降低用户对故障的感知。

# 附　录
（资料性）
系统演进策略

## 1　应用场景分析

向多活信息系统演进的前提是进行业务影响分析，确定采用多活技术的业务范围及其承载系统，然后评估向多活系统演进的可行性。

## 2　业务范围分析

在向多活信息系统演进的业务范围分析中，重点关注如下内容：
——承载重要业务的系统宜考虑采用多活技术。
——重要业务的支撑系统（如重要的认证和加密系统等）宜考虑采用多活技术。
——已经出现处理能力瓶颈的系统，或业务突发性高的系统宜考虑采用多活技术。

## 3　可行性分析

在向多活信息系统演进的可行性分析中，重点关注如下内容：
——是否缺少成熟的多活解决方案和技术组件。
——系统上承载各应用间的耦合程度，以及改造涉及范围。
——迁移至开放平台的业务较容易实现多活。
——可根据系统重要程度依次进行多活演进。
——部分账户型系统对于数据一致性要求较高，建设异地多活的难度较大，集中式系统上可考虑保留一类结算账户及与之结合紧密的应用。
——宜优先采用开放式系统承载新增业务、处理性能有扩展要求的业务、创新型业务（如互联网金融等），以便于后续向多活系统演进。

## 4　演进路线

### 4.1　演进阶段

根据业务发展的不同阶段对金融信息系统业务连续性和灾难恢复的要求，金融信息系统向多活信息系统的演进路线大致会经历如下几个阶段，如图1所示：
——阶段 1：生产系统和数据备份。
——阶段 2：生产系统和灾备系统（同城）、生产系统和灾备系统（异地）。
——阶段 3：生产系统、灾备系统（同城）和灾备系统（异地）。
——阶段 4：多活子信息系统、多活子信息系统（同城）、灾备系统（异地）。
——阶段 5：多活子信息系统、多活子信息系统（同城）、多活子信息系统（异地）。

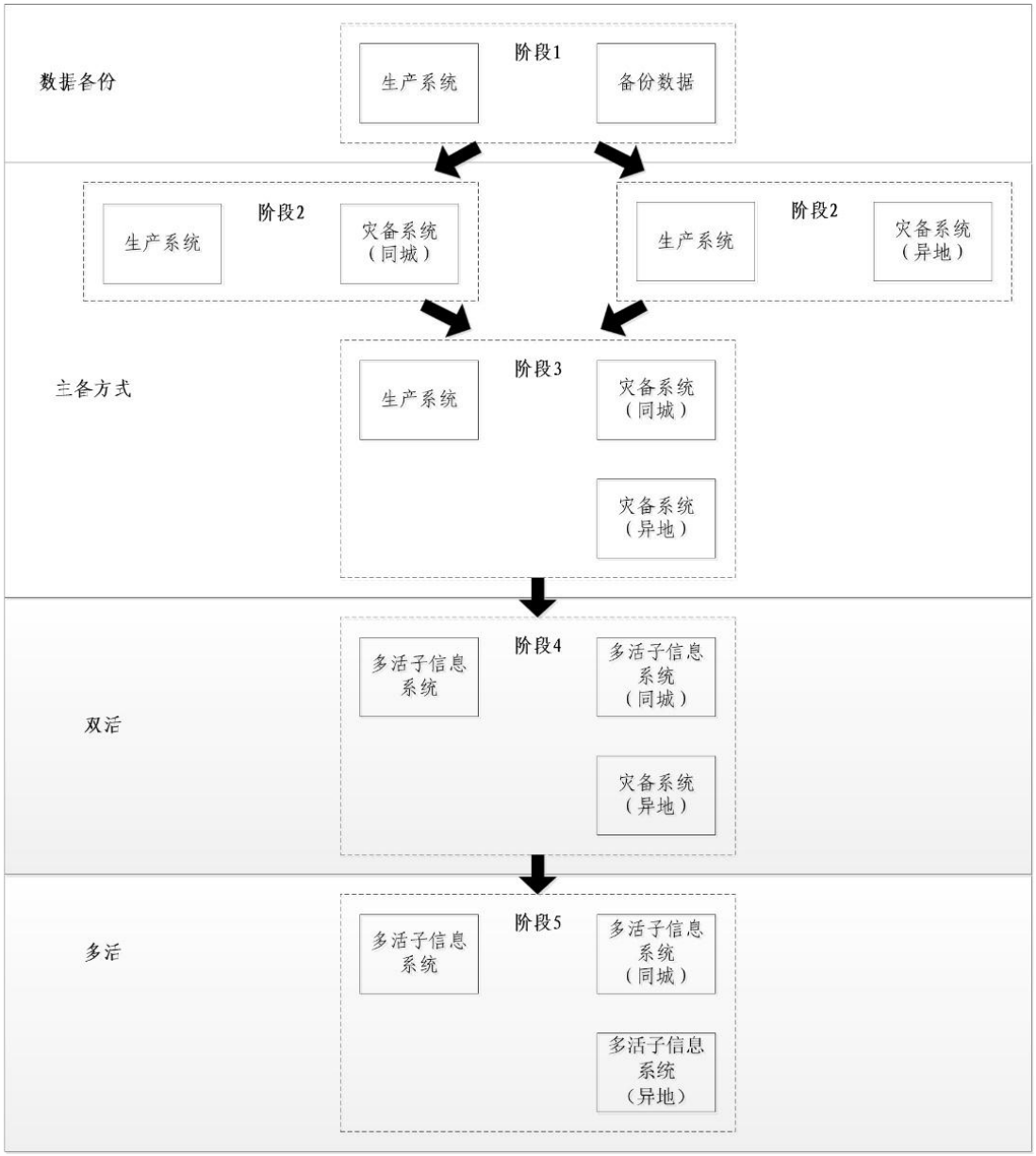


图1 金融信息系统向多活信息系统的演进路线

## 4.2 阶段 1

对系统关键数据进行同城或异地备份。数据备份的周期可是实时或者定期。生产中心发生灾难时，在灾备中心临时部署应用系统，加载关键数据，恢复业务服务。

## 4.3 阶段 2 和阶段 3

在同城或异地中心部署灾备系统，并在生产中心和灾备中心间建立数据同步，同步周期可实时或定期。日常由生产系统提供服务，生产系统发生灾难时，由灾备系统接管服务。灾备系统启动通常包括启用灾备中心系统环境、启动应用、加载数据、连通性验证等工作。

为了提高资源的利用效率，在日常情况下充分利用灾备系统。部分金融信息系统在上述方式的基础上，由灾备系统同时提供查询服务，当发生灾难事件时，由灾备系统接管服务。灾备系统接管服务通常包括暂停数据库异步复制、修改灾备系统数据库状态、启动灾备系统应用环境、流量切换等工作。

### 4.4 阶段 4 和阶段 5

从主备阶段向双活或多活演进的过程需要大量的业务梳理、系统能力评估、业务影响分析、风险分析等相关工作，还涉及到参考前面章节中提出的应用策略实现系统改造，对于不同的业务现状和系统现有架构情况，存在很大的差异。最核心的工作涉及到将原有生产系统上的应用和数据进行拆分，并且根据拆分规则建立新的数据同步关系，同时实现应用并行业务处理相关的改造等，在拆分的过程需要额外注意数据的备份，并且具备出现异常后的回退机制。

假设当前的灾难恢复方式是生产系统、灾备系统（同城）和灾备系统（异地），其向多活子信息系统、多活子信息系统（同城）、灾备系统（异地）演进。以账户型系统为例，可参考如下指南进行拆分工作：

——根据业务梳理情况，明确拆分后的两个多活子信息系统承载的业务范围，假设拆分后各承载50%的账户。

——在生产系统和灾备系统（同城）之间搭建数据同步机制，保证待迁移至灾备系统（同城）的50%账户相关数据在生产系统和灾备系统（同城）之间的数据强一致性。

——完成业务接入和业务处理的改造，实现生产系统和灾备系统（同城）的并行接入和处理功能，且具备相关数据在生产系统和灾备系统（同城）存储的能力。

——启用双活的操作，在这一过程中一般需要短暂的中断业务。调整待迁移至灾备系统（同城）的50%账户相关数据的主备关系（可分多批次进行，如每批次 10%），即灾备系统（同城）启用为主数据，搭建灾备系统（同城）其向生产系统的反向同步复制和设置只读关系，并且在业务接入层和业务处理层完成变更，根据事先规划的拆分规则进行业务接入和业务处理。

——设置灾备系统（同城）与灾备系统（异地）数据的数据复制，保证灾备系统（异地）数据同时对灾备系统（同城）承载业务的数据备份功能。

——由参与方信息系统配合完成迁移流量的路由调整。宜在一段时间内，保证业务流量可从生产系统转发到灾备系统（同城），以避免参与方信息系统将迁移流量范围内的业务流量再发送至生产系统。

——完成上述工作后，原生产系统演进为多活子信息系统，原灾备系统（同城）演进为多活子信息系统（同城），原灾备系统（异地）仍作为备份系统。