ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0208—2021

金融信息系统多活技术规范 参考架构

Multi-active technology specification of financial information system—

Reference architecture

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 参考架构

1 范围

本文件规定了金融信息系统多活技术的内涵、业务视图、架构体系、业务流量分配变更和关键指标设定等内容。

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

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

4.1 驱动因素

在传统金融信息系统灾难恢复中，生产中心与灾难备份中心采用主备方式，其向多活技术演进的驱动因素主要有：

——更高的灾难恢复要求，对于主备方式，当灾难事件发生后，灾难备份系统接管业务往往需要经过较长的时间，而当前金融业务的特点对业务连续性提出了更高的要求。

——接管能力难以把控，对于主备方式，灾难备份系统在正常情况下并不承载真实业务，其真实接管能力难以有效评估，因对其接管能力的评估主要依赖于灾难恢复预案的制定、管理及演练效果，故一旦灾难发生，灾难备份系统是否可接管真实业务难以保证。

——单数据中心扩展受限，由于各方面的限制，单数据中心的扩展能力往往存在瓶颈，或者持续扩展能力的经济效益降低。

——资源利用率低，灾难备份系统在正常情况下不承载业务，资源浪费严重。

——技术提升，主备方式是在传统技术架构的背景下提出的，而云计算、分布式等先进技术的成熟和应用推广，为信息系统灾难恢复能力的升级提供了技术支撑。

——业务覆盖需要，对于覆盖地理范围较广的业务系统，部分用户业务接入的距离过长，可能由于处理延迟带来用户体验的下降。

4.2 灾难备份系统能力比较

多活是信息系统的一种能力。在图1中将多活与传统的信息系统灾难恢复进行比较分析，按灾难备份信息系统的能力将部署方式分为冷备份、热备份、只读、限部分业务、全集业务。

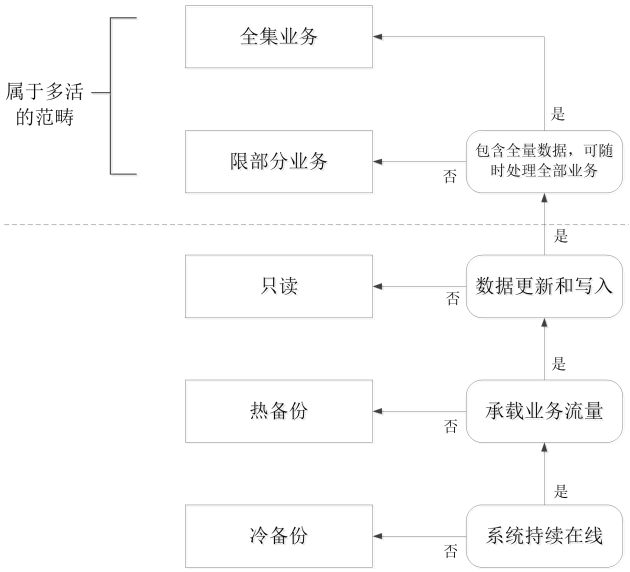

图 1　灾难备份系统能力比较

对于冷备份方式，在正常情况下，灾难备份系统不启动，其与热备份方式的本质区别在于灾难备份系统是否持续在线；对于热备份方式，灾难备份系统持续在线，其与只读方式的本质区别在于是否承载业务（业务中的只读操作部分）；对于只读方式，灾难备份系统在正常情况下只提供查询服务，其与限部分业务方式的本质区别在于是否允许数据更新和写入；对于限部分业务方式，是指在正常情况下，灾难备份系统具备全部的业务功能，但限定只针对全部业务流量的一个子集提供服务，其与全集业务方式的本质区别在于是否针对全部业务流量提供服务；对于全集业务方式，灾难备份系统在正常情况下，即可针对全部的业务功能和全部业务流量提供服务。

对于全集业务方式和限部分业务方式，灾难备份系统是“去中心化”的实现方式，其与生产系统之间并没有明显的主次之分。由于全集业务方式实现难度较大，性价比不佳，业内较少使用。对于限部分业务方式，在正常情况下，生产系统和灾难备份系统均具备全部的业务功能，可通过设定一定的并行策略，约定和控制生产系统和灾难备份系统分别承载部分流量；在灾难发生时，部分系统发生瘫痪，只会影响其承载的部分业务流量，其系统只要具备快速接管业务的能力，仍可做到较小的业务中断，保障业务连续性。

全集业务方式和限部分业务方式属于本文件中描述的多活范畴。

5　多活内涵

5.1　多地理节点部署信息系统

信息系统部署在多个地理节点，各地理节点的位置选择宜综合考虑电力、网络、供水等基础设施的容灾因素，包括独立的空调、电力设施、计算、网络、存储等物理资源。

5.2　布局模式

根据地理节点的相对位置不同，多活信息系统的布局模式可分为同城多活（布局模式）和异地多活（布局模式）。

5.3 业务并行多点接入

各多活子信息系统同时支持业务接入，并支持灵活调整业务接入的多活子信息系统，部分地理节点的灾难和故障不影响其他地理节点上多活子信息系统的业务接入。

5.4 业务并行多点处理

各多活子信息系统同时支持处理业务逻辑，并支持灵活调整处理业务逻辑的多活子信息系统，部分地理节点的灾难和故障不影响其他地理节点上多活子信息系统的业务处理。

5.5 数据并行多点存储

各多活子信息系统同时提供数据存储，且保证其他多活子信息系统存在与业务处理结果一致、可用的数据副本。部分地理节点的灾难和故障不影响其他地理节点上多活子信息系统的数据存储。

5.6 部分业务影响和及时完成业务接管

当某个多活子信息系统发生灾难或故障时，只有部分业务受到影响并需要分配到其他多活子信息系统进行处理。当发生非区域性灾难时，同城多活子信息系统可及时接管业务；当发生区域性灾难时，异地多活子信息系统可在较短时间内接管业务。

6 业务视图

图2中给出了多活信息系统的业务视图，描述了参与方信息系统与多活信息系统之间的业务交互方式。参与方信息系统不需要关注多活信息系统的内部工作方式，只需要通过网络（依据具体的业务要求可能使用专线或互联网）接入多活信息系统将业务流量接入多活信息系统的多个多活子信息系统。在业务流量分配上，多活信息系统的多个多活子信息系统作为一个整体承载全部的业务流量，可根据参与方信息系统与多活信息系统约定的策略，将业务流量分配到多个多活子信息系统。

在图2 a）中，假设所有业务流量可分割为B_1、B_2，直至B_n n个集合。参与方信息系统通过多活子信息系统S_1处理属于集合B_1的业务流量，通过多活子信息系统S_2处理属于集合B_2的业务流量，以此类推，通过多活子信息系统S_n处理属于集合B_n的业务流量。

当参与方信息系统发现某个多活子信息系统不可用时，需要将原来通过该多活子信息系统处理的业务流量分配到其他多活子信息系统。这里所指的多活子信息系统不可用，是多活子信息系统对于参与方信息系统而言的整体不可用（如数据中心整体故障或者网络专线故障），如某个多活子信息系统可部分工作，且其仍可将业务流量转接至其他多活子信息系统进行处理，可不需要参与方信息系统变更业务流量的分配。在图2 b）中，多活子信息系统S_1不可用，参与方信息系统将属于B_1的业务流量分配到多活子信息系统S_2至多活子信息系统S_n中的一个或多个上进行处理。

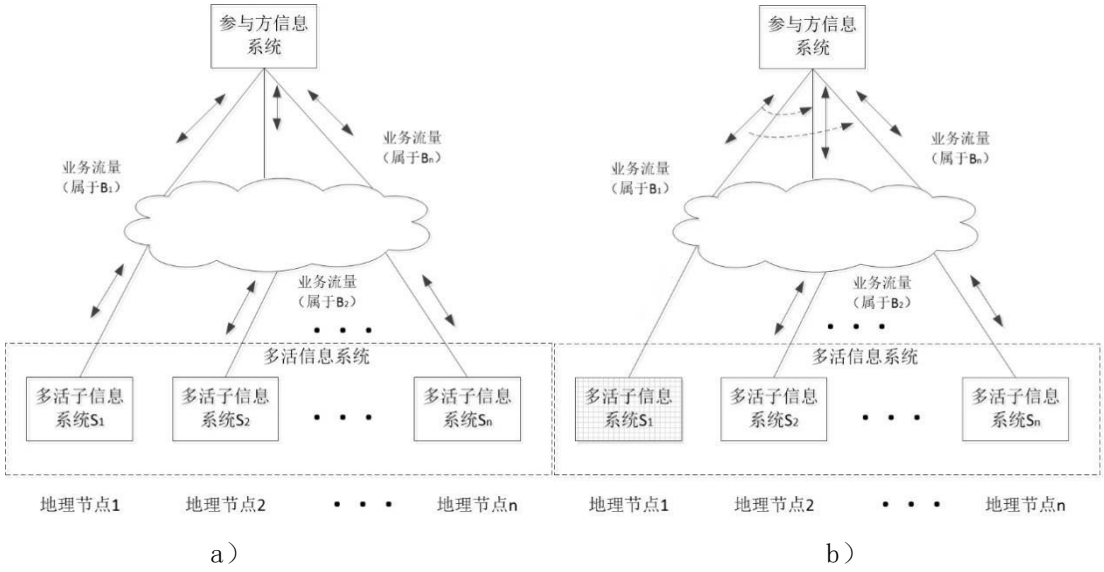

图 2　多活信息系统业务视图

7　多活架构体系

7.1　多活架构体系概述

多活信息系统通常拆分为业务接入层、业务处理层、数据存储层，见图 3。业务接入层主要负责业务多点接入和灵活路由，将业务流量按照一定的路由策略发送至业务处理层；业务处理层负责业务逻辑处理，并调用数据存储层功能实现数据读、写；数据存储层负责接收业务处理层的调用进行数据持久化操作，实现数据的多点读、写功能。

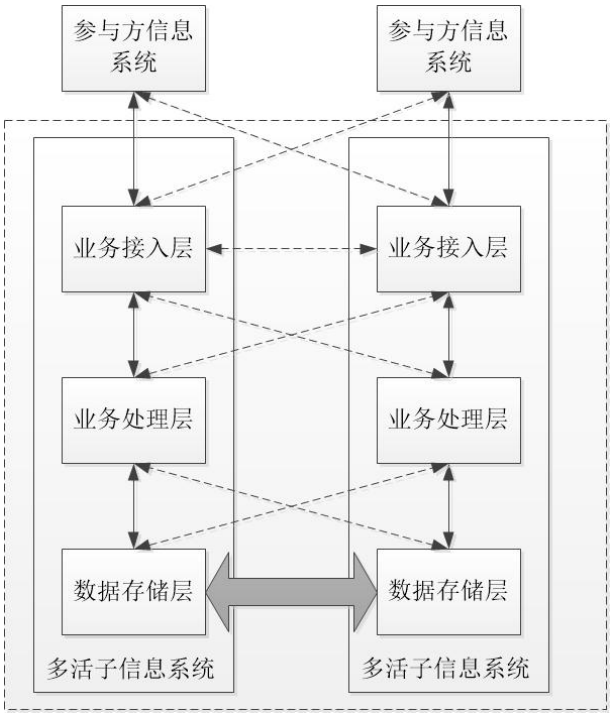

图 3　多活架构体系

7.2 接入要求

在发生灾难和某些故障（如网络故障等）等场景下，多活子信息系统可能无法将其接收到的业务请求转发到其他多活子信息系统，这种情况下，需要接入多活信息系统的参与方信息系统将业务流量分配到正常工作的多活子信息系统。参与方信息系统接入多活信息系统方面的要求如下：

——参与方信息系统应接入两个或两个以上的多活子信息系统。

——对于参与方信息系统为多活信息系统的，参与方信息系统应至少有一个多活子信息系统接入两个或两个以上的多活子信息系统，参与方信息系统其余的多活子信息系统中应至少有一个接入一个多活子信息系统，宜选择其他多活子信息系统未接入的多活子信息系统。

——对于参与方信息系统为主备方式的，生产系统应接入两个或两个以上的多活子信息系统，备份系统应至少接入一个多活子信息系统。

——对于参与方信息系统从多点发起业务请求的，应将参与方信息系统的多点均接入两个或两个以上的多活子信息系统。

——在多活子信息系统不可用时，参与方信息系统应保证及时将业务流量分配至其他接入的多活子信息系统。

——应保证对于某个接入路径不可用时，其余接入路径具有足够的网络带宽和业务处理能力接管故障接入路径的业务流量。

——应支持对参与方信息系统进行分级分类，设置差异化的接入要求，如接入专线数量、接入专线隔离要求、接入专线网络能力、业务流量分配变更时间等。

——接入不同多活子信息系统的网络链路宜具有相同的链路特征，如网络带宽、传输时延等。

——应保证不因参与方信息系统的业务流量分配变更造成网络地址冲突等问题。

——参与方信息系统与多活信息系统之间宜建立指令交互机制，参与方信息系统根据多活信息系统发出的指令，执行预先约定的操作。

——参与方与多活信息系统应定期开展切换演练，以保证某个多活子信息系统不可用时，可将原来通过该多活子信息系统处理的业务流量分配到其他多活子信息系统。

7.3 业务接入层要求

业务接入层要求如下：

——应支持参与方信息系统同时接入两个或两个以上多活子信息系统的业务接入层。

——应支持将业务流量发送至两个或两个以上多活子信息系统的业务处理层，支持按路由策略对接入的业务流量进行路由选择；对于业务流量转发至异地多活子信息系统的情况，可通过异地多活子信息系统的业务接入层间接转发。

——应支持对路由策略进行实时控制。

——应保证某个多活子信息系统发生灾难或故障时，其他多活子信息系统具有足够的业务接入能力，在较短时间内接管原由其接入的业务流量。

——应支持根据业务逻辑实现用户的业务流量路由的一致性，或通过与业务处理层协同工作以规避路由不一致对业务处理结果的影响。

——设备应冗余部署，避免设备单点故障对业务接入的影响。

——网络线路应冗余部署，避免单条线路故障对业务接入的影响。

——应支持自动切换或集中切换功能，当出现参与方信息系统与业务接入层之间故障、接入层内部故障、接入层与业务处理层之间故障、业务处理层故障时，可自动或集中切换路由，保障业务流量发送至可用的业务处理层。

——应支持对大于当前业务接入能力的业务流量进行限流，避免对多活信息系统造成影响。

7.4 业务处理层要求

业务处理层要求如下：

——应支持同时处理多个多活子信息系统业务接入层转发的业务流量。

——应保证某个多活子信息系统发生灾难或故障时，其他多活子信息系统具有足够的业务处理能力，在较短时间内接管原由其处理的业务流量。

——设备应冗余部署，避免设备单点故障对业务处理的影响。

——网络线路应冗余部署，避免单条线路故障对业务处理的影响。

——应满足业务处理的无状态要求，具体包括：

- 多个多活子信息系统的业务处理层应用之间解耦，不存在依赖关系；
- 业务处理层将单次业务的处理结果发送至数据存储层存储；
- 业务处理层处理单次业务请求不依赖其他业务请求，业务处理过程中只使用来自单次业务请求携带的信息以及数据存储层存储的信息。

——应满足业务处理的幂等性要求，即单次业务请求与多次重复业务请求的处理结果一致，不因多次重复业务请求而产生不同的处理结果。

7.5 数据存储层要求

数据存储层要求如下：

——应支持同时处理多个多活子信息系统业务处理层的数据存储请求，或者支持处理其他多活子信息系统数据存储层的数据复制请求。

——应保证某个多活子信息系统发生灾难或故障时，其他多活子信息系统具有足够的存储能力接管原由其存储的数据量。

——业务数据应在多个多活子信息系统的数据存储层存在数据副本。

——对有数据一致性要求的数据，应在同城多活子信息系统具有满足数据强一致性的副本，应在异地多活子信息系统具有满足在较短时间内达成数据最终一致性的副本。

7.6 监控功能要求

监控管理要求如下：

——应具备多活信息系统全局的健康度检查功能，包括：

- 应监控各个多活子信息系统的健康度信息（如处理时延、成功率等）；
- 当某个多活子信息系统的健康度下降到预先设定的阈值，则可触发策略，将全部或部分业务交由其他多活子信息系统接管；
- 当达到监控阈值时，应支持自动通知运维人员，如通过邮件、短信、电话等方式。

——应具备对各多活子信息系统的监控功能，包括：

- 应支持对各多活子信息系统的基础设施、业务接入层、业务处理层、数据存储层的运行状态分别进行监控；
- 应支持设定阈值，可根据监控情况触发业务接入层、业务处理层、数据存储层内部和各层之间的自动切换；
- 当达到监控阈值时，应支持自动通知运维人员，如通过邮件、短信、电话等方式。

——应建立多种监控机制，且各种监控机制相互隔离，且在部分监控机制失效时其余监控机制仍可监控到重大故障事件。

——应通过监控功能为灾难恢复和切换决策提供依据，应在保证准确度的同时，尽量降低切换决策的时间。

——宜支持根据业务需求对切换决策的策略进行动态调整。

——监控功能本身应具备高可用特性。

8 业务流量分配变更

8.1 分配变更过程

在多活技术中，灾难和故障时进行业务分配变更的前提和基础是满足第7章中提出的架构体系要求。其他要求如下：

——应支持灾难和故障发生时处理中的业务的核对，并根据业务需求对处理中的业务进行妥善处理。

——应支持受灾难和故障影响的多活子信息系统可靠的重新接管业务，如逐渐增加接管业务流量等。

——应考虑计划内业务流量分配变更（如日常维护、系统变更等场景）和计划外业务流量变更（如灾难和故障等场景）的差异。

8.2 分配变更演练

分配变更的演练要求如下：

——应针对部分多活子信息系统发生灾难、故障及相关的恢复进行模拟，并对多活信息系统的业务分配变更能力和其他多活子信息系统业务接管能力的有效性进行验证，验证内容应包括但不限于功能、性能和业务连续性保障能力。

——应针对多活信息系统的业务接入层、业务处理层、数据存储层发生故障及相关的恢复进行模拟，并对多活信息系统其他部分的有效性进行验证，验证内容应包括但不限于功能、性能和业务连续性保障能力。

9 多活关键指标设定

多活信息系统的关键指标包括多活业务集中度、多活同城业务集中度、多活业务接管时间、多活数据恢复点目标、多活接管容量能力，这些关键指标共同决定了多活信息系统应对灾难的能力。

多活关键指标定义如下：

——多活业务集中度：用于衡量业务在各个多活子信息系统之间的分散程度，降低多活业务集中度可降低单一多活子信息系统灾难或故障的业务影响范围。例如：多活业务集中度为25%，其可能实现方式是部署4个多活子信息系统，并且在各多活子信息系统间平均分配业务接入流量、业务处理流量和数据存储量，当任何一个多活子信息系统发生灾难或故障，受影响的业务均不超过全部业务的25%，其余的业务不受任何影响。

——多活同城业务集中度：用于衡量业务在各个不受同一区域性灾难影响的地理区域间的分散程度，降低同城业务集中度可降低区域性灾难的业务影响范围。例如：多活同城业务集中度为50%，可能的实现方式是两个地理区域分别部署两个多活子信息系统，并且在4个多活子信息系统间平均分配业务接入流量、业务处理流量和数据存储量；其他可能的实现方式是双活信息系统，两个多活子信息系统部署在不同的地理区域，平均分配业务接入流量、业务处理流量和数据存储量。对于上述两种实现方式，均满足任何一个区域性灾难发生后，受影响的业务不超过全部业务的50%，其余的业务不受任何影响。

——多活业务接管时间：用于衡量灾难发生后，对受到影响的多活子信息系统业务流量重新分配并由其他多活子信息系统接管的时间。降低多活业务接管时间，可减少灾难引起的业务（部分业

务）的中断时间。

——多活数据恢复点目标：用于评价当发生灾难或故障时，多活信息系统中受影响的数据应恢复到的时间点要求。

——多活接管容量能力：用于衡量灾难发生后，多活信息系统承载受影响业务的能力，可用多活信息系统能承载受影响业务的百分比表示。例如，设定在单一多活子信息系统故障时，其他多活子信息系统可接管100%的业务；设定对于任何区域性灾难，其他多活子信息系统可接管其50%的业务。为了达到上述要求，需要合理分配多活信息系统的冗余容量，同时还要考虑冗余容量在各个多活子信息系统之间的分布，以及冗余容量在不同地理区域之间的分布。

参 考 文 献

[1]GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范

[2]JR/T 0044—2008 银行业信息系统灾难恢复管理规范

[3]ISO/IEC 20933：2016 Information Technology—Distributed Application Platforms and Services (DAPS)—Access Systems

[4]中国人民银行.《中国人民银行办公厅关于印发<中国人民银行信息系统业务连续性分级保障标准（试行）>的通知》（银办发〔2017〕92号），2017年4月18日