

安小信金融贷后 AI 专业深讲稿

专业技术与商业价值客户版

杭州安小信智能科技有限公司 2026 年 10 月 11 日文案精修版 v5

让金融资产进入 AI 自主经营时代

从个贷贷后智能语音服务切入，安小信连接策略决策、实时沟通与结果监督，帮助业务团队减少重复联系、完整执行策略，并把每次沟通用于持续跟进资产。

这份材料面向金融机构业务、科技、风险合规和采购负责人。先回答买什么、如何落地、怎样验收，再展开专业数据、模型评测、小脑控制层以及与声网共创的实时 AI 能力。具体启用范围、服务责任和验收标准在项目工作说明书中共同确认。

一 机构需要解决的四类经营问题

第一是事实不连续。名单、通话、承诺、停联和回款分散，作业人员很难知道上一次发生了什么，也难以决定下一次是否该联系。第二是策略执行不一致。优先顺序、事实核验和边界处理依赖个人，既可能漏做合法任务，也可能重复执行不应执行的动作。

第三是过程难以核验。一段录音自然，并不能回答用的什么策略、为什么披露信息、是否允许作出承诺。第四是价值难以归因。呼叫量和口头承诺增加，未必带来真实回款或完整成本改善。

安小信的价值主张是让获授权任务更完整地执行、让例外更容易被识别和复核、让业务结果能够对账。成本改善是其中一个结果，不能用降低规则、过度联系或只挑容易案件取得表面优势。保险及其他金融经营场景可以沿用部分基础能力，但仍需独立业务规则、授权与验证。

二 从一项可验收的业务任务开始合作

首次合作不要求替换机构全部核心系统，也不把完整贷后管理变成一次无边界开发。建议选择一种资产类型、一个主要账龄、一类作业任务、一套权威数据来源和一个责任团队，说明需要改善的主要问题，以及达到什么证据后才值得扩围。

典型交付由共同平台、行业规则配置、必要连接器、限定 FDE 实施与运行支持组成。已有模型、线路或呼叫中心是否可复用，先按接口、授权和服务责任确认。所有对外联系仍需有清楚的业务依据和启用范围，演示成功不是生产授权。

事项	机构需要明确	安小信及联合方需要明确
资产与业务	合同主体 债权或委托关系 联系资格	接入字段 状态来源 使用限制
决策与审批	业务目标 规则负责人 有权批准人	配置版本 工具权限 待复核路径

事项	机构需要明确	安小信及联合方需要明确
数据与系统	用途 保存期限 接口及安全要求	访问控制 隔离 日志与退出处理
运行与异常	投诉停联 争议及后续处置责任	监测 限流 停止 恢复及问题响应
验收与结算	验收人 主要指标 对照和付款条件	交付物 成本边界 计量及证据

技术提供、共同交付与受托运营需要分别定责。合同叫什么不能替代谁实际签约、联系、审批、处理数据和承担结果。合作伙伴有助于进入客户，但伙伴的准入资格不会自动转移给其他主体。涉及司法等专业处置，由有资格且获授权的主体履行职责。

三 从适配诊断到付费验证再到生产扩围

先用标准体验和一次范围明确的适配交流确认是否合适。客户只需提供脱敏概况：资产类型、主要账龄、当前流程和痛点、现有系统，以及业务、数据合规、预算三类负责人。此阶段不要求上传真实资产包，不通过官网表单提交债务人信息。

进入验证前，双方确认固定范围和付费工作说明书。写清样本及排除条件、主指标、控制底线、接口数量、所需工时、期限、客户配合事项、交付物、验收和退出。POC 是一项有范围的验证服务，不默认等于全年生产合同，也没有适用于所有客户的统一年费。

合作阶段	核心产物	进入下一阶段的依据
适配诊断	需求与责任边界 采购路径	真实问题 有权联系人 预算可能性
固定范围付费验证	同口径业务效果 控制与技术证据	双方验收 缺陷关闭 明确经济性
生产服务	已批准范围内持续运行	使用质量 服务责任 收款与稳定性
受控扩围	增量规模或新能力	容量 成本 授权与新增验收通过

验证不通过时，按合同修复、缩小范围或退出，保留结果和数据处置记录。不能为了赶转产改变样本、删除不利结果或事后调整主要指标。生产之后增加规模不等于自然增加所有能力，新系统、新账龄和新业务目标仍需评估。

四 从客户的一句话理解业务机制

以下为模拟：某笔早期逾期案件处于可联系状态，任务目标是核身后确认情况并了解还款安排。任务先引用资产来源、余额核验时间和批准策略，拨前重查联系资格、时段、频次、暂停标记和状态变化。

客户说昨天已经还款。系统把这句话记录为客户陈述，不直接修改到账事实；若获准查询权威回款来源，则查询并标记核验结果。来源不可用时，按机构规则进入待核验，暂停不适宜继续的动作，记录需要有权人员处理的事项。只有权威来源确认后，才能更新到账或结清状态。

客户询问是否能减免一半。系统可以解释获准的申请流程、记录意向，但不能自行批准金额，也不能在语音里先作保证。执行记录应显示触发了什么规则、哪些动作被阻止、采用哪个版本的回应，以及后续如何核验。自然表达、控制判断和事实修改是三个不同环节。

五 全生命周期管理要求状态连续

M1、M2、M3 反映账龄，已联系、承诺待履行、待核验、争议、暂停及结清反映作业状态。账龄决定适用策略的一部分，但不能覆盖刚刚发生的新事实。同为 M1，有有效承诺的案件和长期未取得联系的案件，不应接受相同普通外呼。

资产事实 → 当前状态 → 本次目标 → 获批策略 → 执行结果 → 权威核对 → 下一步任务

每次状态变化都保留来源、时间、操作者或系统事件以及适用版本。承诺金额与实际到账分开，争议与欠款事实分开，暂停联系与退出管理分开。重复事件不制造重复任务，迟到事件也不能覆盖更晚的有效状态。

短账龄重点是合法任务覆盖、策略完整执行与履约；长账龄重点是有有效联系、争议处理和连续管理。后续专业处置可以衔接状态与材料，但不代表安小信自动获得相关资格。必要上下文按批准的用途和期限留存，支持跨账龄连续跟进。

六 让每项任务带着目标和权限执行

给 Agent 的不只是一条 Prompt，而是一份任务书：资产事实及出处、本次目标、策略版本、可披露范围、核身要求、工具权限、需批准事项，以及结束和异常条件。模型负责理解和表达，不能因为提出了建议就获得执行权限。

拨前控制检查当前状态、联系资格和停止条件。关键字段未知、过期、权限不明或查询失败时，先阻止不满足条件的任务。工具调用校验参数和范围，结构化结果校验合法值，重试保持幂等。下游接受请求、实际接听、完成任务和核验到账分别记录，不能合并成一个成功标记。

一条可复盘的证据链连接任务、事实快照、策略及模型版本、权限判断、外部请求、供应商回执、实际事件和权威结果。业务人员可以解释为什么做，工程人员可以定位哪里失败，管理人员可以追到谁应处理。记录本身也要控制访问和保留期限，不能为了审计无限复制个人信息。

七 把行业数据转化为专业判断

四类数据分别管理：权威资产事实用于当前判断；制度和知识用于业务解释；获准样本用于学习与评测；执行和回款用于验证结果。数据持有不自动等于可训练，客户授权生产处理也不自动允许跨客户复用。每批资料先确认控制方、处理方、用途、期限和退出处理，再做最小化提取、脱敏、去重和质量检查。

专业标注覆盖核身、有效联系、客户明确表达的意愿与能力、争议、承诺金额日期、投诉停联、策略执行以及后续履约。标签要能回到对应片段、案件、来源和标注版本。已还款陈述不能标为真实到账，情绪识别不能替代真实意思，更不能作为施压依据；无法确定时保留未知。

指南为每个标签给出定义、正反例与边界，关键标签采用抽检、双人复核和分歧仲裁。评估同时看准确率、漏识别、标注一致性和长尾覆盖，而不是仅看总样本数。困难样本进入受控改进流程，保留谁复核、修改了什么和怎样验证。

可向客户展示的是获准用途、去重口径、质量覆盖、版本和独立评测改进。迁移记录数、通话分钟或历史业务规模都不能直接改写成自有训练规模。对未获训练授权的数据，系统仍可在明确授权范围内检索或执行业务，但不将其混入通用训练资产。

八 RAG 策略 提示与训练分别起作用

能力层	主要作用	必须检查的依据
RAG 检索	取回当前任务允许使用的知识	来源 权限 新鲜度 检索命中与引用
策略与权限	规定适用动作及必须满足的条件	规则版本 审批 生效范围
提示优化	改善任务理解 表达和输出结构	模板版本 回归结果 场景切片
监督微调	在明确训练范围内调整模型行为	数据授权 训练记录 独立评测

新增制度通常先更新知识与规则，不必每次重训；实时资产事实通过权威接口核验，不靠模型记忆。哪一层发生问题就定位哪一层，避免把所有改进统称为训练。检索失败、事实过期和模型不知道时，应采用既定降级，而非补出一个看似合理的答案。

生产数据、训练集、开发集和冻结测试集分别设置用途及访问域。同一案件、客户或高度重复对话跨集合会使记忆冒充泛化，因此要按案件、机构和时间隔离，并按账龄、语言噪声和风险类别建立测试切片。高风险任务另外设对抗和边界用例。

评测既看业务完成，也看虚构事实、越权、漏核身、遗漏停联和异常处置。增加样本、检索或规则后，用同一冻结测试和必要消融比较判断增益。报告保留样本范围、排除规则、分母、版本与失败样例；总体均值不能掩盖关键少数场景退化。

九 小脑检查回应与动作并及时干预

小脑是策略和安全控制层的解释性名称，不是天然不会犯错的第二模型。动作门检查当前业务状态、身份、权限及工具参数；输出门检查候选表达的事实依据、敏感信息和越界承诺。两条路径分别判定，动作被禁止时，语言也不能先替它作出承诺。

业务状态与授权 → 动作门与输出门 → 允许 替换或阻止 → 执行回执与结果核对

确定性规则适合核验权限、范围和已知硬边界；风险识别模型辅助发现上下文风险。被控制的 Agent 不能自行修改控制配置。规则服务不可用、判断超时或状态不一致时，需要事先规定停止、限定文本或待复核等默认动作，而不是自动放行。

实时干预要区分停止新任务、停止生成、清空待播音频和远端实际停止播放。前者成功不能证明后者发生，已播出的声音也无法撤回。输出前检查与风险发生后的干预分别验证；分句审查还要处理跨片段含义、缓存和流式竞态。

验收保留触发时点、候选输出、规则版本、控制请求、供应商响应及媒体侧结果，测量风险发生到实际停止的 P50、P95 和 P99 延迟，同时报告漏拦、误拦和超时。断网、重复命令、回执迟到及恢复后重放也要测试。具体组合未联调验收前，不把接口存在写成生产能力，更不承诺绝对合规。

十 与声网共创实时通信与对话式 AI

安小信与声网围绕金融贷后场景共创实时通信与对话式 AI 能力。共创重点是把实时互动、对话编排和声音体验与资产状态、任务目标、策略权限和结果回流连接起来，而不是简单并列两个品牌。

声音输入 → 声学与轮次处理 → ASR → 业务决策及模型编排 → 输出检查 → TTS → 声音输出

声学处理、网络、语音识别、业务查询、模型推理和合成共同决定端到端表现。客户插话、短暂停顿或提出核验要求时，应按明确的场景策略安排话轮与回应。关键事实表达、核身和异常处置不能只追求低延迟，声音自然也不应被用来隐瞒 AI 身份或诱导客户。

Agora 官方文档提供主动中断及指定文本播报接口，可作为受控对话的执行支点。[1][2] 指定播报接口对 mlm 配置存在限制，不把级联模型路径的能力直接套到所有端到端方案。供应商接口能力、联合架构设计和客户部署启用分别核验。

项目中需确认线路、实时互动、模型服务和安小信业务层各自的责任、日志、故障处理和服务保障。联合效果以明确测试及客户验收证明；知识产权、品牌和商务分工以协议为准，不新增未约定的排他或独占承诺。

十一 通话内执行与通话后迭代

通话内根据新事实和已批准规则执行，通话后从异常、错误与复核反馈形成改进候选。两者不是同一权限：正在运行的 Agent 不能边执行边批准自己的新规则或把客户谈话自动加入训练集。

例如金额异议被重复误判，先区分 ASR、标签、知识或策略问题，再修正对应层。候选版本保留模型、提示、知识、策略、数据与测试版本；冻结测试通过后小范围验证，观察风险、任务效果和运行成本，再按批准范围发布。发生回归能够恢复前一版本。

客户应能解释同一个问题为什么在新版本中处理不同。共性能力回到产品主干，客户专属事实和规则保持隔离。现场经验形成可复用产物，而不是每个客户拥有一套无法维护的分支，这也是交付周期和后续成本可改善的基础。

十二 FDE 交付与运行安排

FDE 从责任、数据和接口开始，完成字段映射、来源验证、授权配置、测试用例与运行看板，再执行限定上线。客户业务负责人确认目标，数据和合规负责人确认用途与规则，安小信承担约定的软件及支持，供应商和机构人员按职责参与异常处理。FDE 不能代替客户作业务授权。

每次交付至少留下版本清单、接口映射、规则及权限配置、验收记录、异常处理责任、恢复回滚与退出安排。变更前核对生效范围与兼容性，恢复时核对状态和重复事件，避免旧任务重放或多系统重复联系。

部署形态按数据与采购要求确定，可以讨论机构环境或约定服务环境，但不承诺所有形态已经交付。访问最小化、用途隔离、日志保护、凭据管理和留存删除都纳入项目设计。真实数据先通过客户批准通道，演示与外部市场材料不接收生产个人信息。

扩围分为已验任务增量、配置差异和新能力开发。每类变更确认数据与权限变化、工时、运行成本、支持容量和新增验收。优先复用平台主干、行业规则及连接器，新增定制单独批准，不让一次 POC 长期承担免费产品开发。

十三 验收先确定主指标和共同分母

不同账龄选择不同主要指标。M1、M2 可以在固定观察期比较回收率或恢复正常率；长账龄可以比较有效联系、争议处理和持续管理质量。一次验证先约定一个主要业务结果，辅以效率指标，不在看到结果后改成最有利的指标。

样本、分层、随机或匹配方法、观察期和排除条件预先冻结。长账龄可联率以初始符合联系条件的去重借款人为分母，不用拨打次数替代人数，也不让新增样本随意改变分母。回款使用权威核验数据，区分自然回收、历史催收影响与本方案可能带来的增量；前后对比存在季节、资产和政策差异时不直接声称因果。

验收维度	核心观察	必要证据
业务效果	主指标与固定观察期 同分层比较	样本清单口径 权威回款 对照方法
控制底线	核身 授权 停联 投诉及越权处置	规则用例 失败样本 完整处理记录
工程质量	可用性 尾部延迟 幂等 恢复	端到端测试 监测 供应商及媒体回执
完整成本	技术 线路 实施 人员和运行	同范围成本表 使用计量 工时记录

重大控制缺陷不允许用更高回收或通话量抵消。具体控制底线与接受阈值应在项目开始前由有权人员确定；模拟体验只证明演示路径，不能代替生产验收。

十四 客户价值和规模怎样测算

客户净价值看同范围的经核验收变化，扣除包括安小信收费在内的完整运营成本变化。若把效果增加与成本节省同时计算，需要说明各项是否已经包含，避免双计。人工保留、复核、质检、线路、AI、FDE、系统改造和异常处理都不是免费资源。

传统服务预算可按互斥分层的本金、同观察期回收率及对应合同费率求和。不同账龄和服务范围的回收率与费率不能交叉混乘，服务预算也不等于安小信收入。客户版不以任意预算份额推导产品报价，项目定价按实际范围、能力和责任讨论。

管理规模区分累计导入、期末管理和月均有效付费在管。持续经营观察可用每日有效授权、生产付费且承担约定任务的去重本金形成月均值，排除重复委托、试验和已退出资产。合法暂停联系但仍有监测责任，不必等同于退出管理；同一资产跨系统镜像不能多计。

生产扩围之前一起检查客户价值、缺陷关闭、机构责任、支持容量和预算。先让一个边界清晰的单元成立，再扩大资产、账龄和业务场景，避免把未验证的预期当成批量采购理由。

十五 下一次专业交流如何推进

首轮交流围绕五个问题展开：谁负责这项业务，当前最重要的问题是什么，哪一个系统提供权威事实，什么结果才算通过，以及预算和采购如何决策。安小信自有 BD 持续推进需求、合同、验收与续约；合作伙伴按明确贡献提供引荐、联合售前或交付能力，而不是替代客户判断。

建议由业务、科技和数据合规负责人共同参加一次适配会，先用脱敏概况确定一类资产、一个目标和责任边界，再决定是否形成付费验证工作说明书。无需预先上传真实资产明细、录音或身份证件。

产品体验号码为 952-3900，体验时段 08:00 至 20:00；官网为 <https://anson.xin>。体验以模拟场景为主，不提交真实个人金融信息。演示、商务诊断、正式验证与生产使用是不同阶段，须分别确认范围和授权。

资料与技术来源

产品机制依据安小信专业材料，合作方向依据联合会议纪要，项目启用以验收确认。

[1] Agora 官方文档 Interrupt the agent mid response，页面更新 2026 年 8 月 7 日，本次核阅确认中断接口说明。
<https://docs.agora.io/en/ai/build/shape-the-conversation/interrupt-agent>

[2] Agora 官方文档 Broadcast a message using TTS，页面更新 2026 年 9 月 25 日，本次核阅确认指定播报和 mllm 适用限制。
<https://docs.agora.io/en/api-reference/api-ref/conversational-ai/speak>