

Architect

SACC

2022 中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2022

· 激发架构性能 点亮业务活力

云上会议 网络直播 | 2022年10月27-29日

IT168.com

ChinaUnix.net

ITPUB

金融级系统海量流量下的高可用架构道与术

京东科技 . 康杨

不可用

- ◆ 什么是不可用？
- ◆ 不可用的本质？
- ◆ 多长时间不可用？
- ◆ 通用的高可用方案？
- ◆ 高可用方案的考虑因素？
- ◆ 数字化时代的高可用？

什么是不可用?

已知
未知



不可用



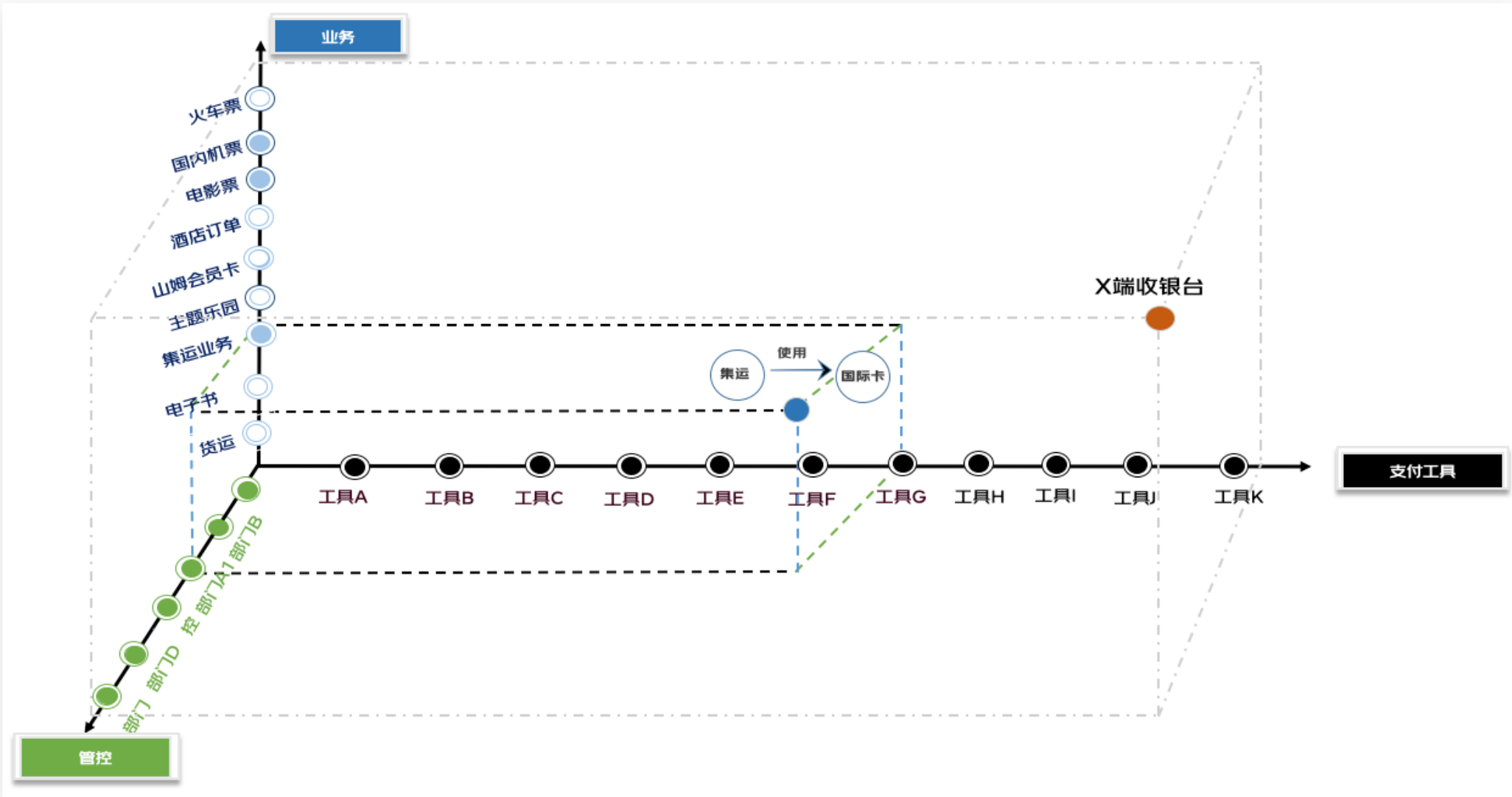
条 件



时间
人

不可用是指潜在风险在一定条件触发下的结果呈现

复杂业务的可用性挑战





信息泄露

- 信息盗取：木马病毒、假冒网站、数据安全事故
- 信息泄露：身份信息、账号密码泄露



账号盗用

- 账号接管：登录、修改及管理身份、绑卡、窃取信息数据、动账转账



交易欺诈

- 盗刷
- 套现
- 盗帐号交易
- 线上业务交易欺诈



营销作弊

- 帐号垃圾注册
- 积分作弊套现
- 羊毛党团伙
- 虚假交易



信贷欺诈

- 身份冒用/非本人申请
- 身份美化
- 多头共债
- 现/资金用途
- 恶意逾期/恶意失联

不可用的本质

系统的本质

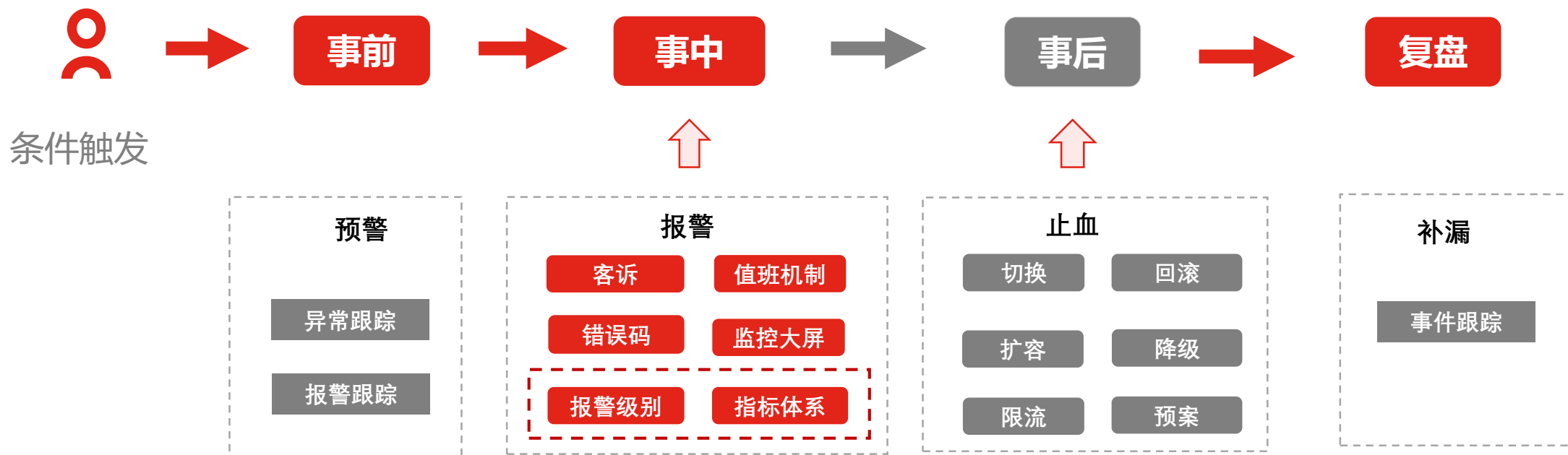
基于对 **业务本质** 理解进行的 业务建模(结构), 并使用 **编程语言** 表达这些 模型,
在空间和时间限制下将它们映射成 **机器语言**

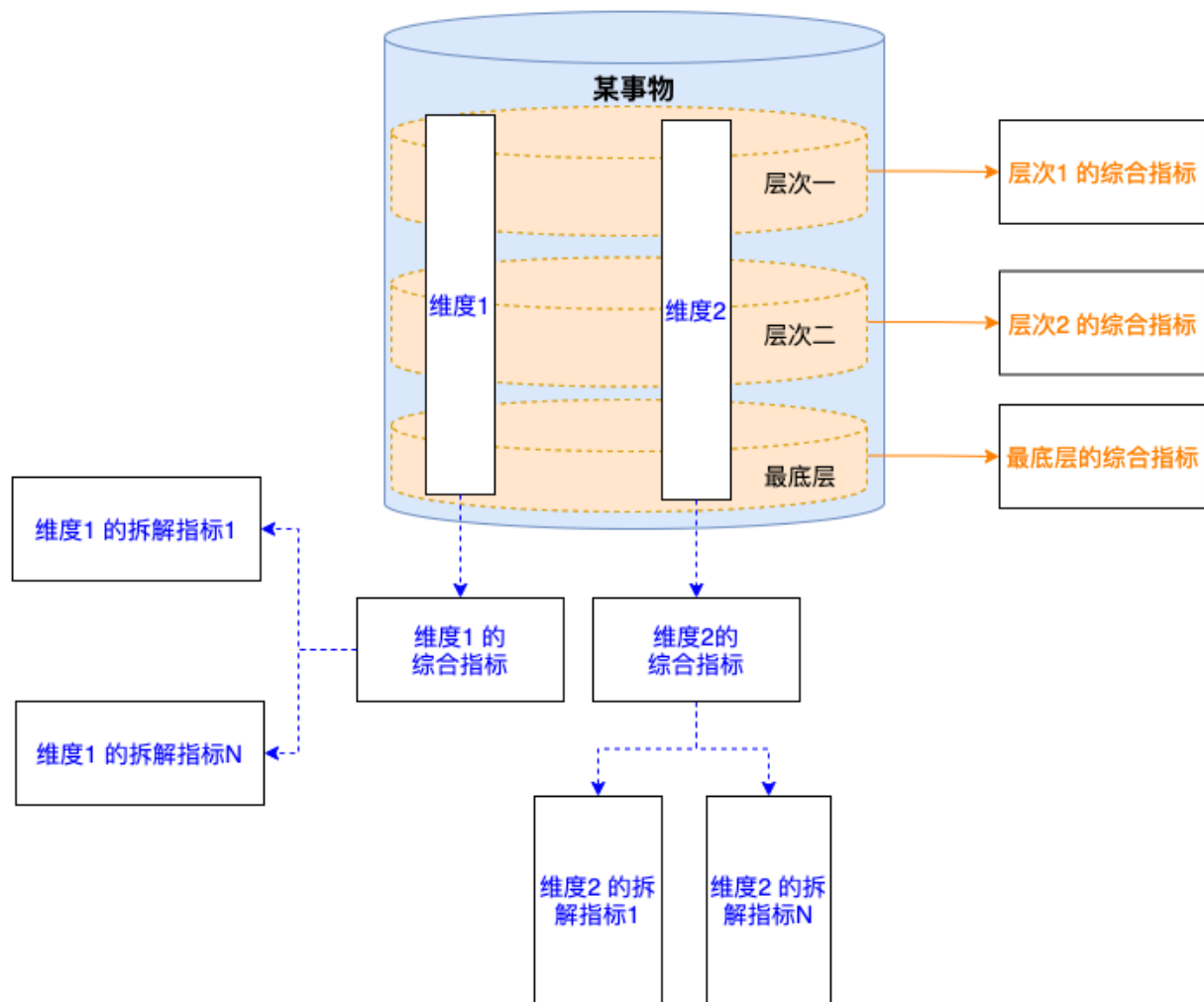
不可用的本质

- ◆ **业务模型**的不可用
- ◆ 技术实现的不可用

可用性最大的挑战来自于，我们有限的认知以及世界无限的变化，和我们不知道我们不知道

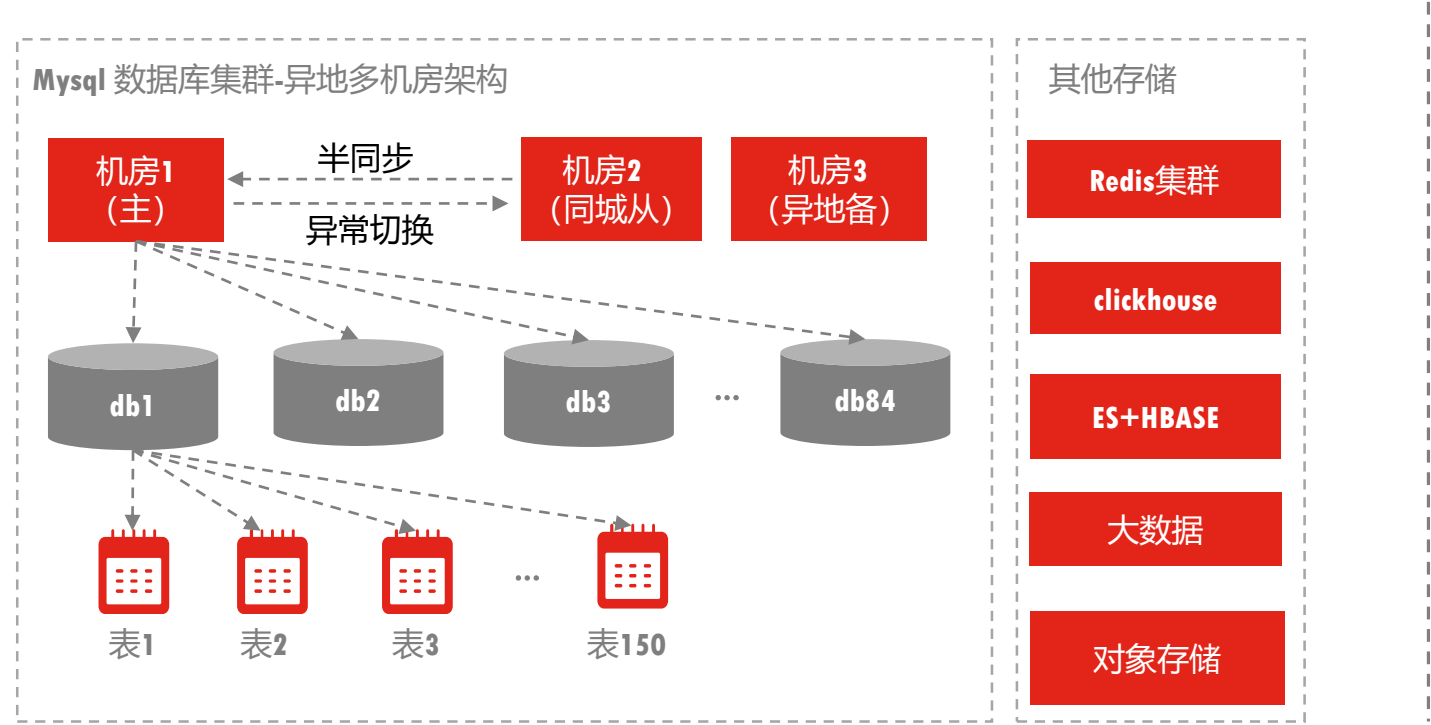
线上服务体现 **业务价值**，持续稳定的运行是一切的前提，时间是影响 **业务连续性** 的关键因素



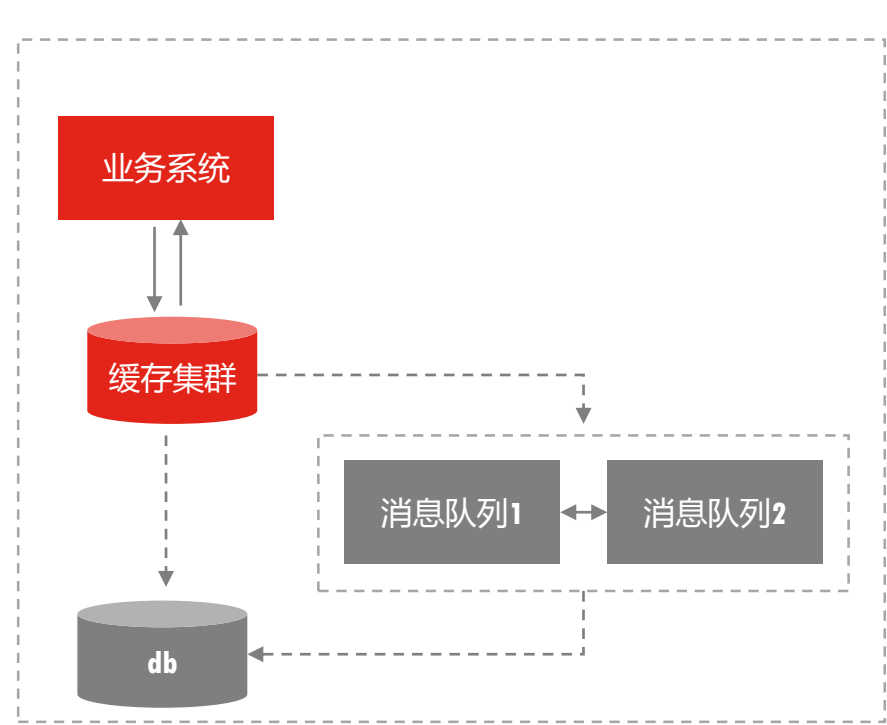


基于 MySQL 自身高可用，以及一定的容灾设计（如热备、读写分离、冷热分离、内存DB、延时异步入库等），最终达到数据库整体架构的高可用

强依赖数据库架构

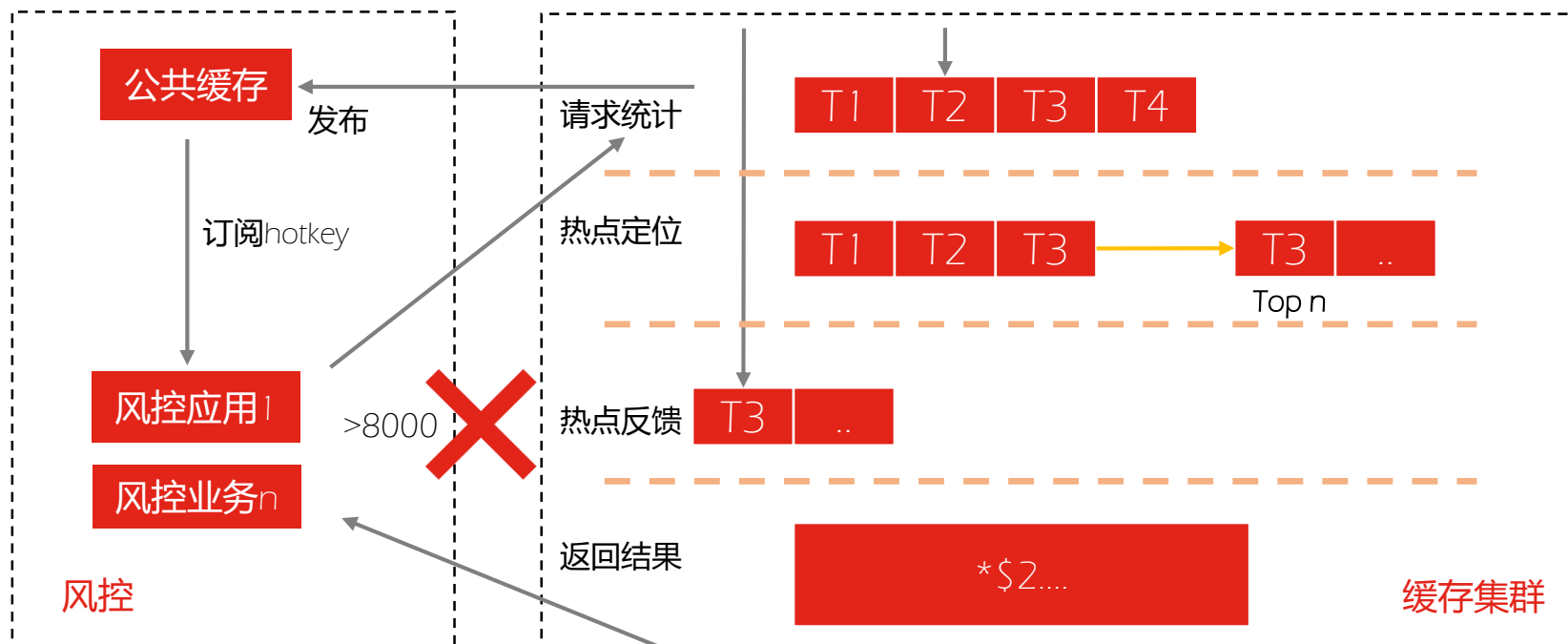


弱依赖数据库架构



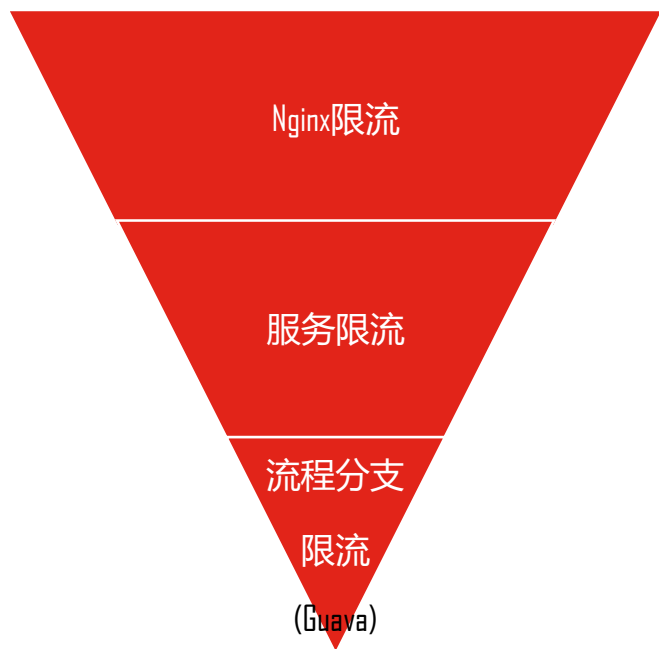
防刷作为对抗恶意流量的常用方式，将影响降至最低

发现恶意用户或恶意机器人，并禁止其高频、单一访问



系统承载的流量总有上限，超出上限很容易造成宕机甚至雪崩

◆ 请求级限流



分层、逐层限流

Provider限流策略

Provider限流为服务端IP限流

* 方法: 方法为必填项

* 别名:

* 类型: default(加锁阻塞式计数)

* 次数限制: 50

* 窗口时长: 1000ms

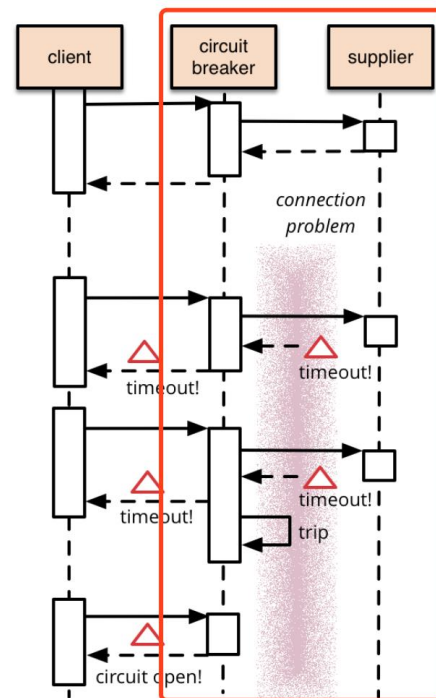
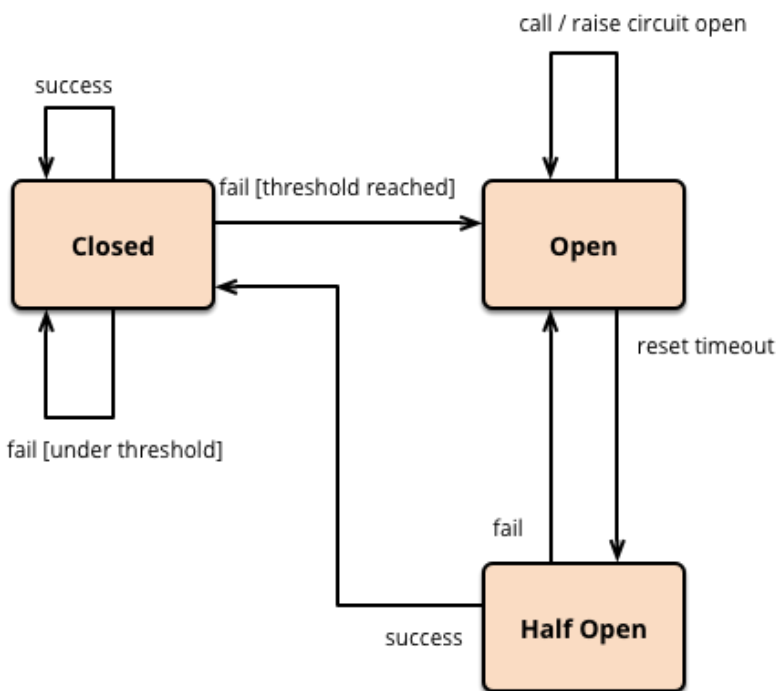
* 生效: ☒ 否 ☐ 是

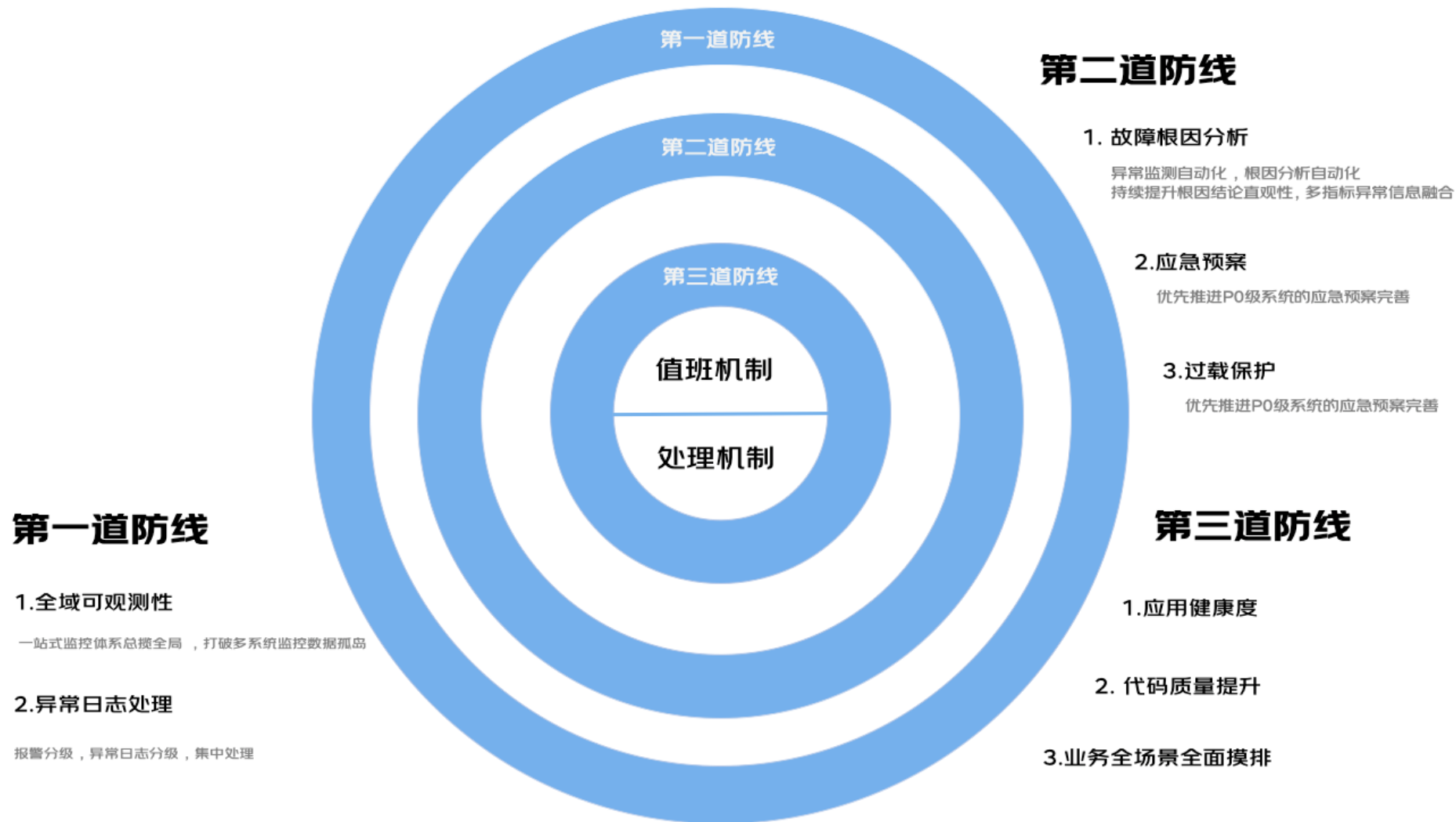
取消 确定

基于令牌桶服务端限流

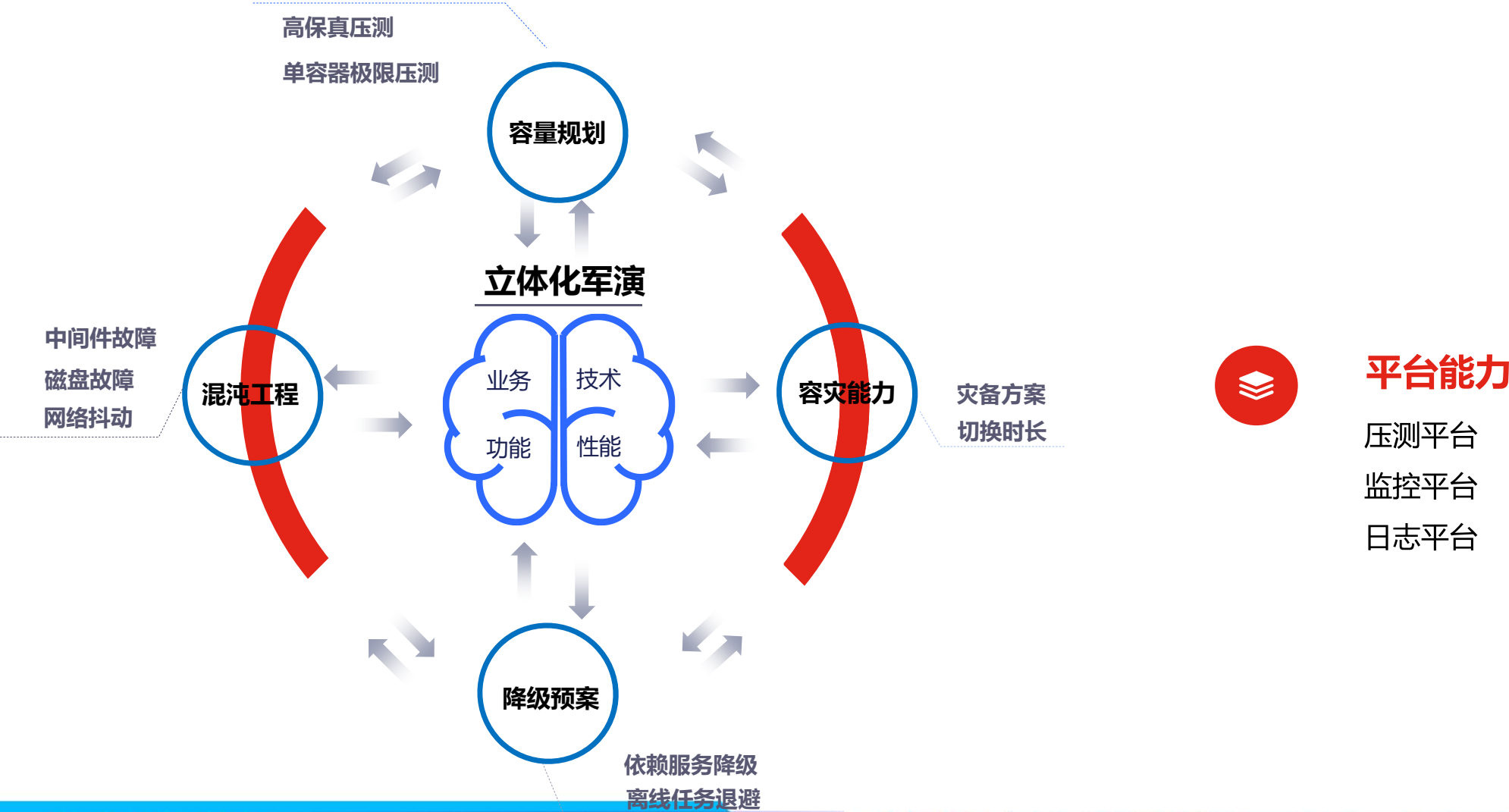
◆ 会话级限流

降级的本质是 **取舍**，当依赖的接口出现问题时，为 **保证基本服务、或重要服务可用**，需及时切断与故障接口
的请求，避免引发 **雪崩** - 普通降级 & 应急预案



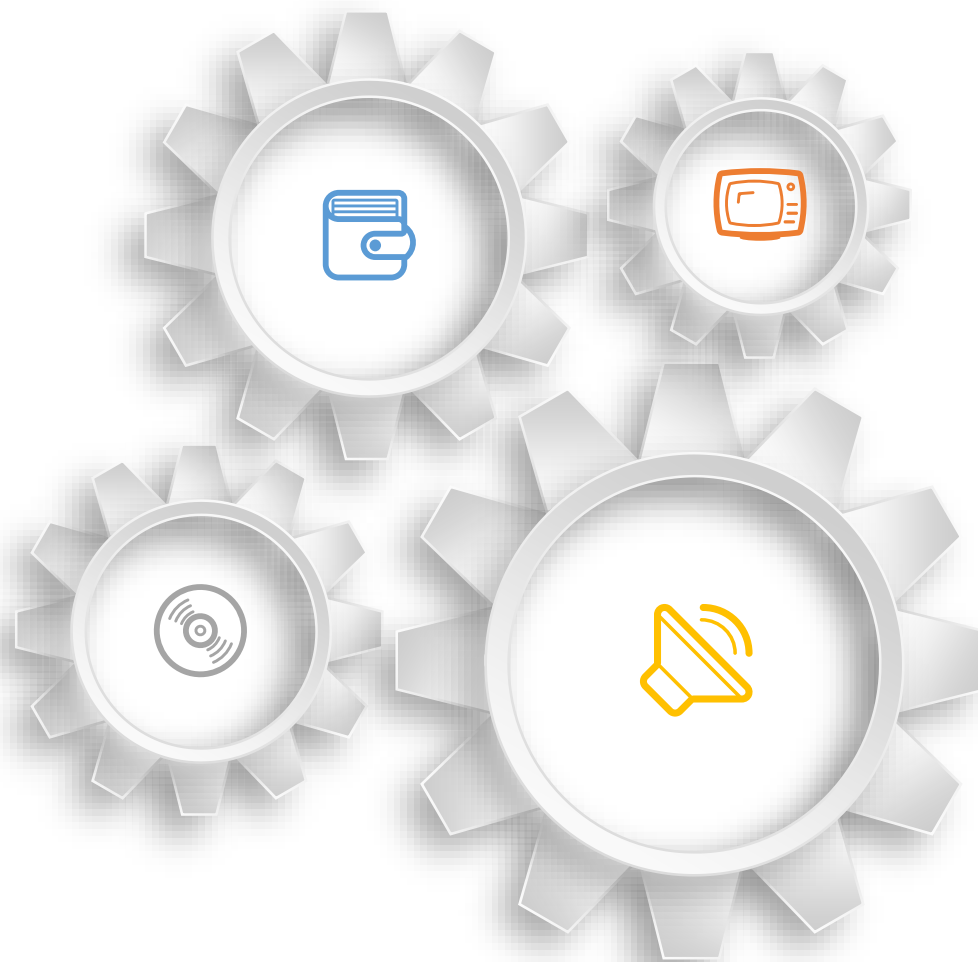


高可用 - 立体化军演



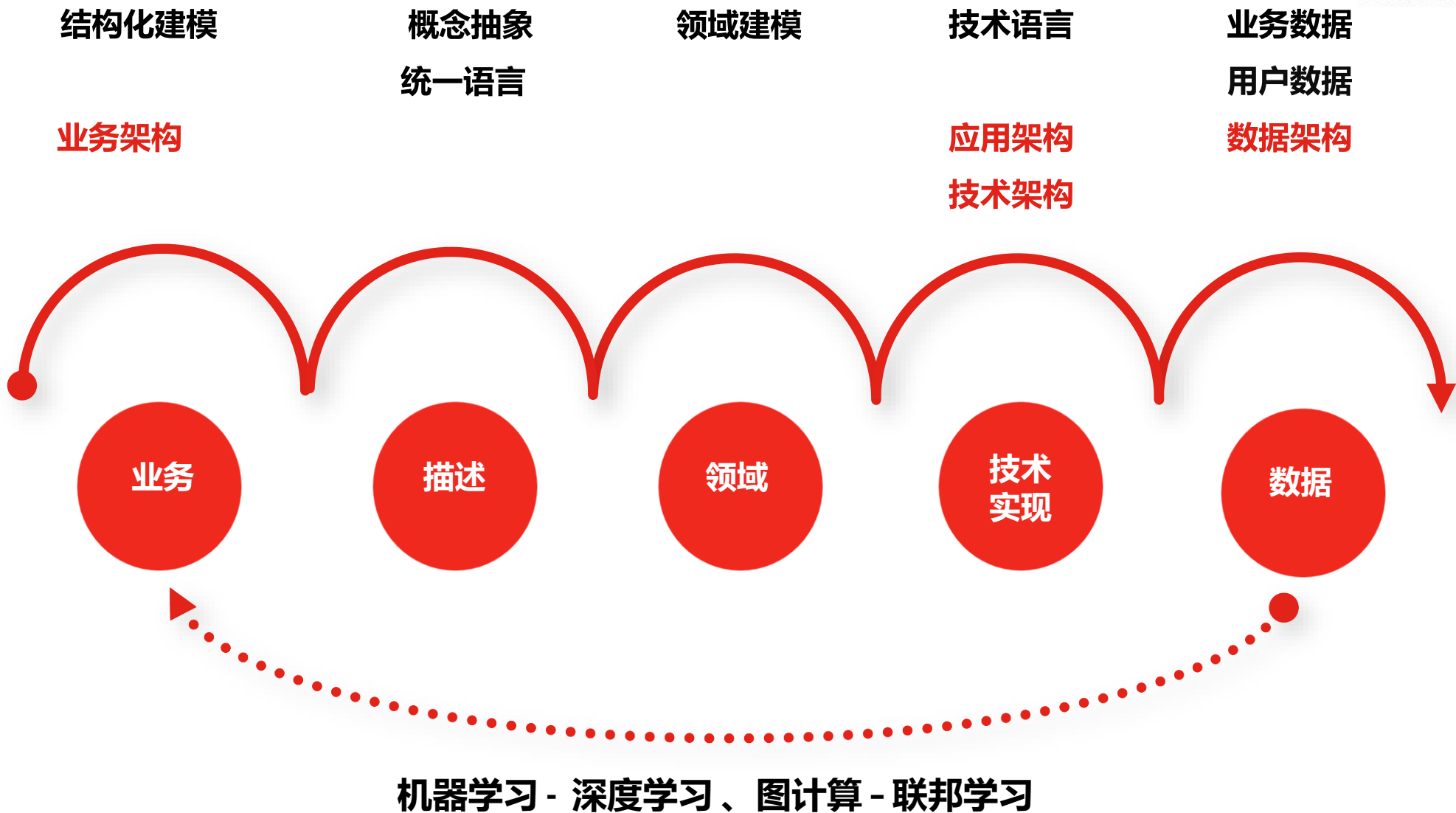
- 成本
- 研发成本
 - 管理成本
 - 资源成本

时间



用户体验

全局的视野







THANKS

Architect