QCon
全球软件开发大会

百度大规模微服务架构下的
故障全面预防
精细止损
深度观测

甄真

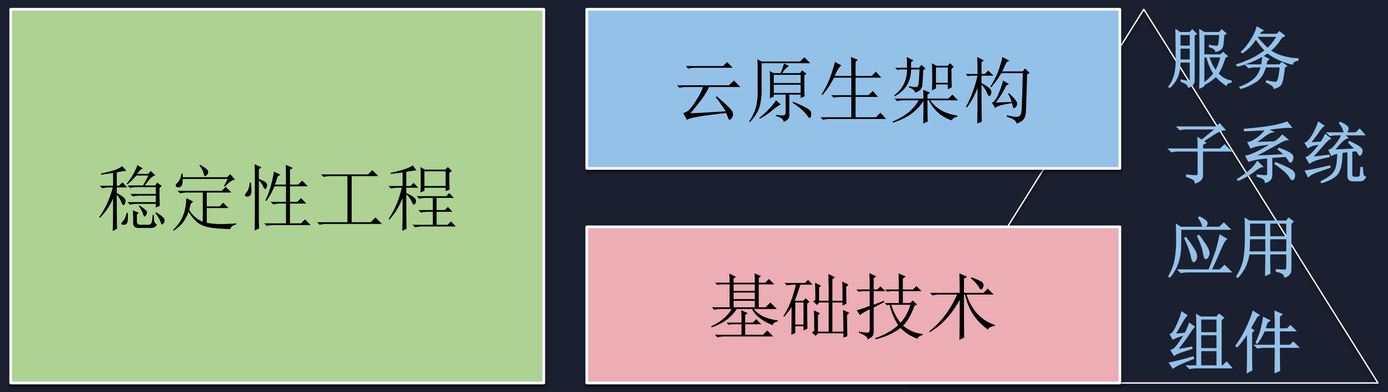
个人介绍

履历

2013：加入百度搜索团队
2013-2016：负责搜索核心模块的业务架构
2016-今：负责搜索全系统架构优化

现在

搜索稳定性团队技术负责人



背景

- 微服务架构
  - 服务多
  - 拓扑复杂
  - 依赖多
  - 迭代频繁

故障产生概率大

背景

故障典型症状——拒绝

目标：尽最大努力服务好每一个query，减少拒绝

query：今天天气怎么样？

百度搜索系统

很抱歉，您要访问的页面不存在

高可用挑战

“数”说百度搜索系统的复杂性

可用性要求

N0万台机器

N大地域

N00种服务

N0 PB数据

N0万变更/天

N00种故障

N00人参与

N0亿PV/天

极端严格

参照表

系统可用性	不可用时间/年
90%(1个9)	36.5天
99%(2个9)	3.65天
99.9%(3个9)	8.76小时
99.99%(4个9)	52.56分
99.999%(5个9)	**5.26分**
99.9999%(6个9)	**31.54秒**

百度搜索系统介绍

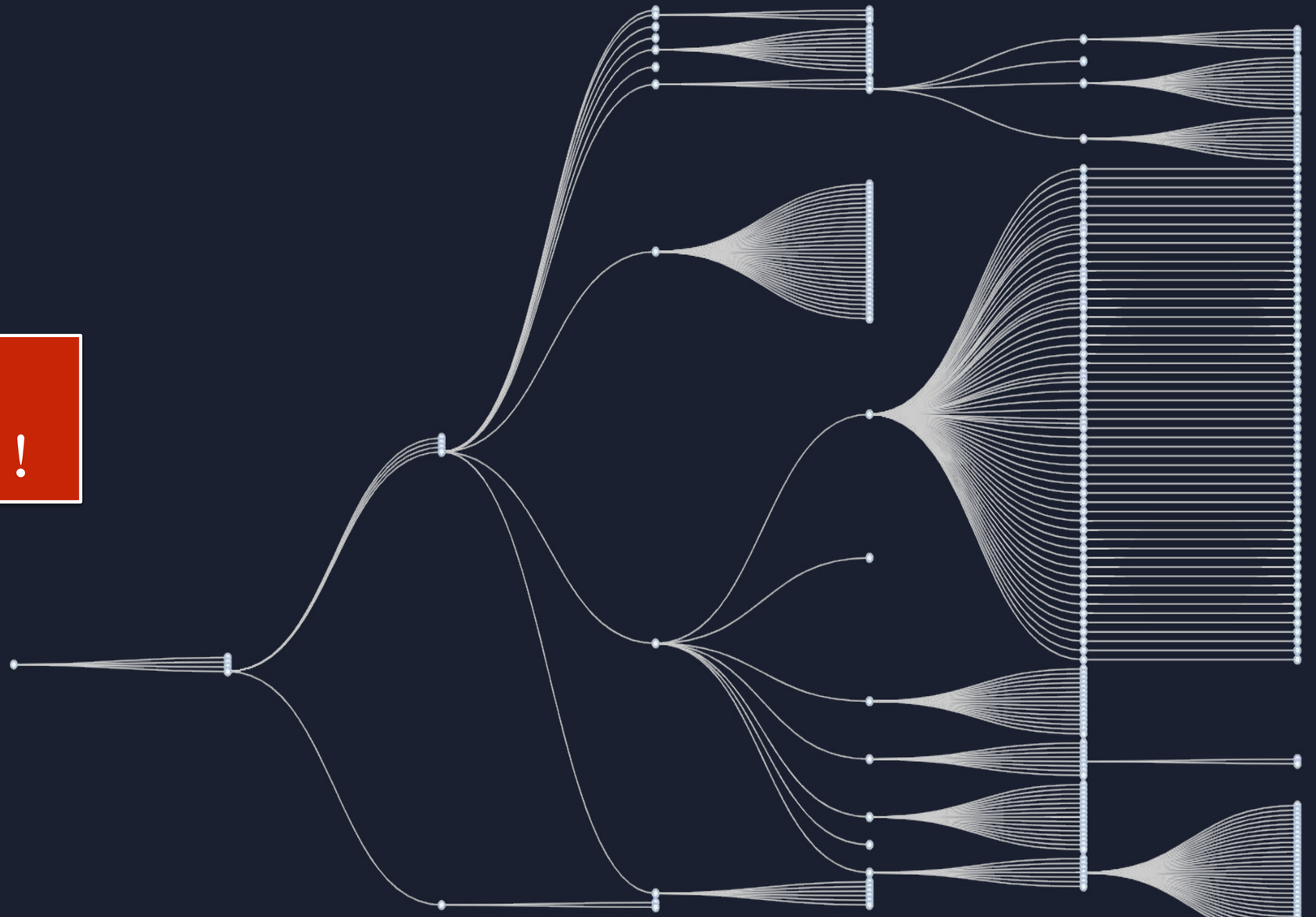
一个query在搜索系统的处理过程

节点多 → 异常概率大

拒绝
是一件多么容易发生的事！

$$0.99999^{10000} = 0.9$$

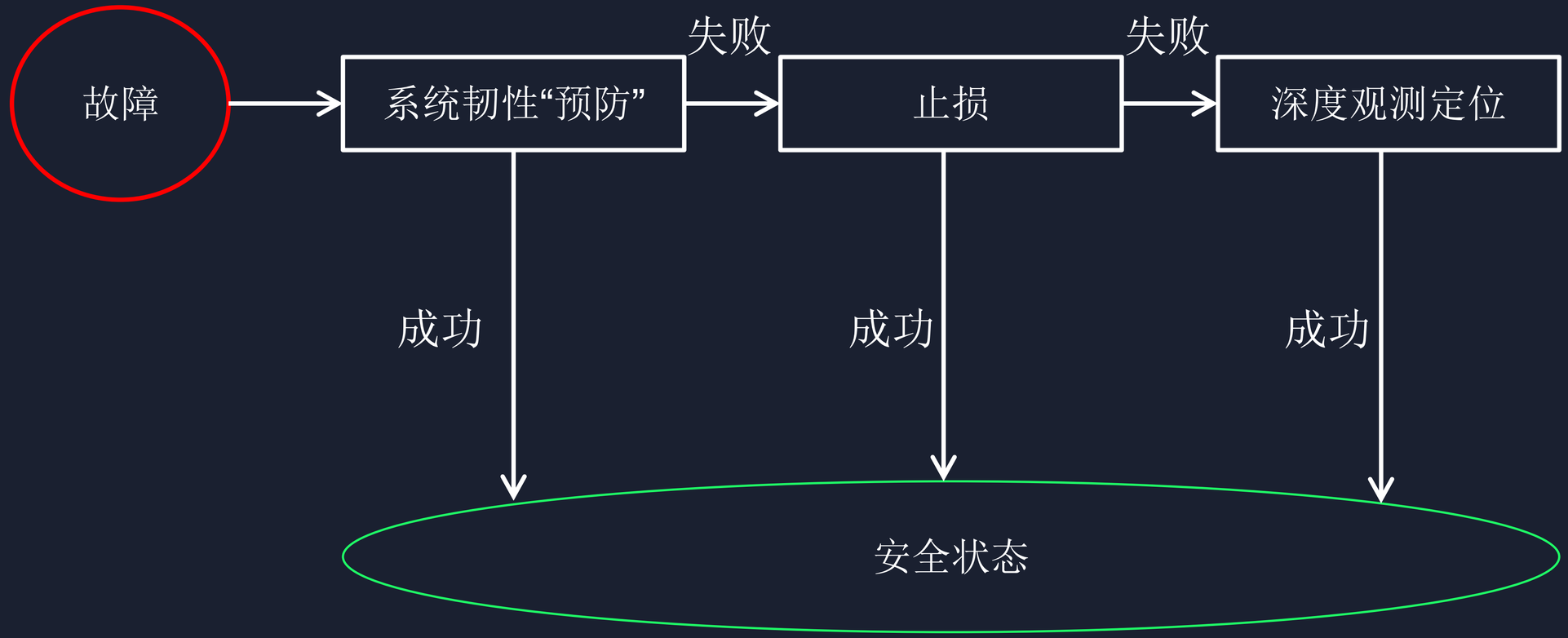
$$0.999999^{10000} = 0.99$$



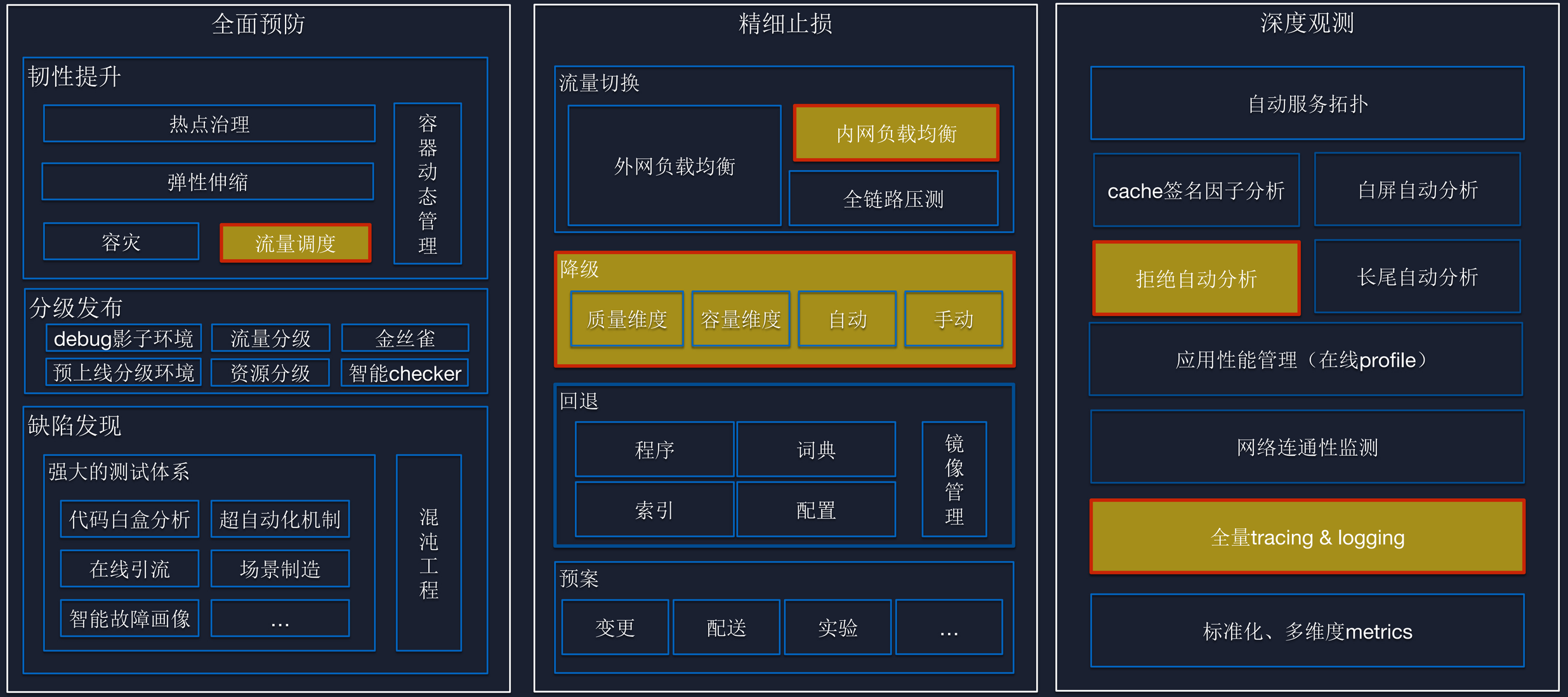
query经历“一斑”（1/X000）

故障处理过程

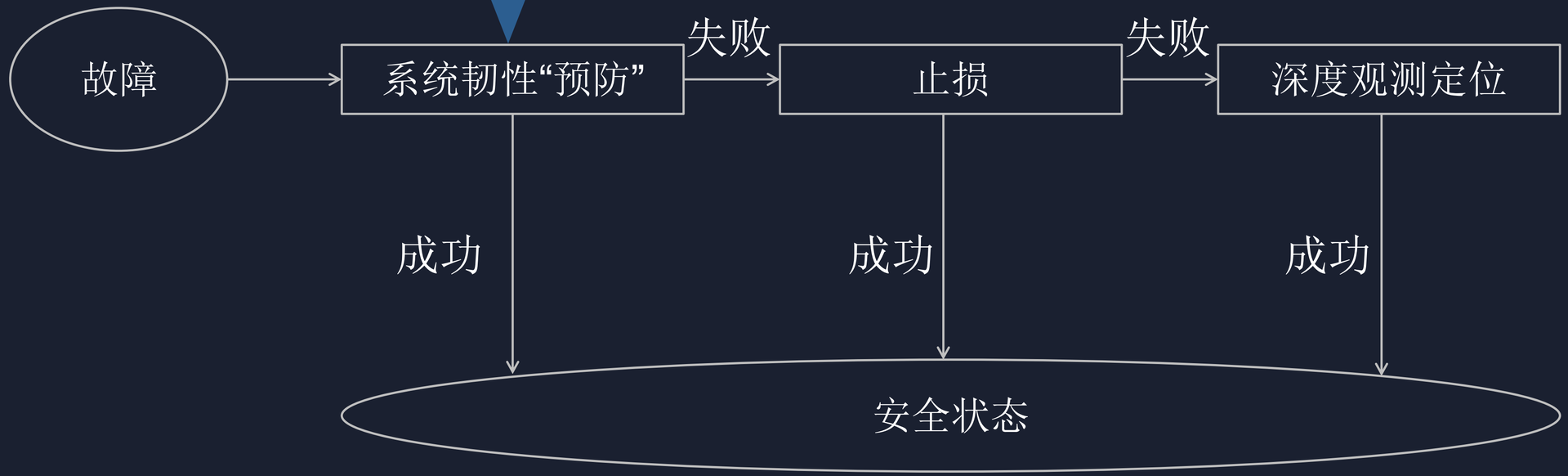
永远不要指望故障不发生，必须把故障当作常态



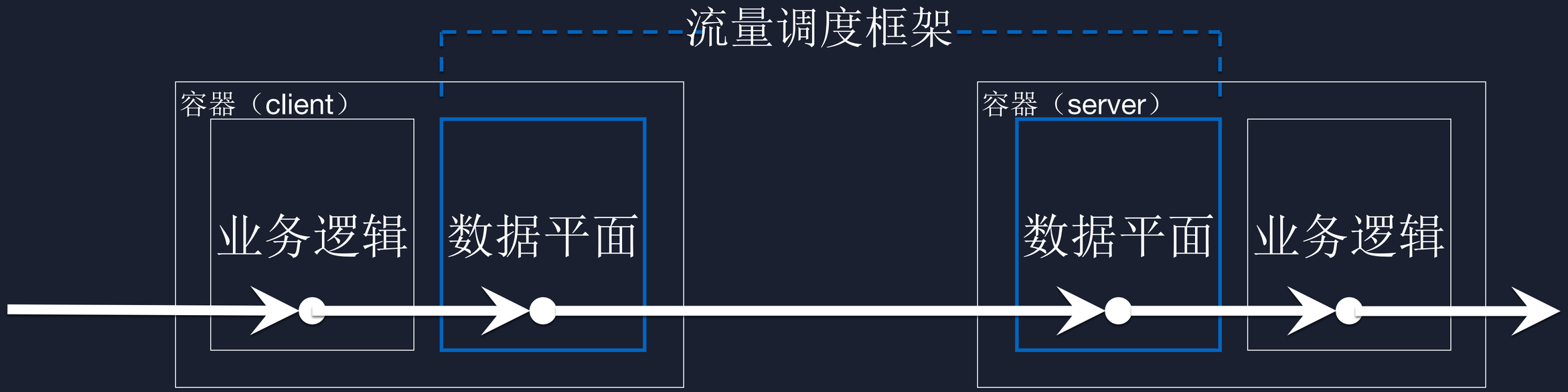
百度高可用技术栈


全面预防
韧性提升
热点治理
弹性伸缩
容灾
流量调度
容器动态管理
分级发布
debug影子环境
流量分级
金丝雀
预上线分级环境
资源分级
智能checker
缺陷发现
强大的测试体系
代码白盒分析
超自动化机制
在线引流
场景制造
智能故障画像
...
混沌工程
精细止损
流量切换
外网负载均衡
内网负载均衡
全链路压测
降级
质量维度
容量维度
自动
手动
回退
程序
词典
索引
配置
镜像管理
预案
变更
配送
实验
...
深度观测
自动服务拓扑
cache签名因子分析
白屏自动分析
拒绝自动分析
长尾自动分析
应用性能管理（在线profile）
网络连通性监测
全量tracing & logging
标准化、多维度metrics

全面预防——流量调度

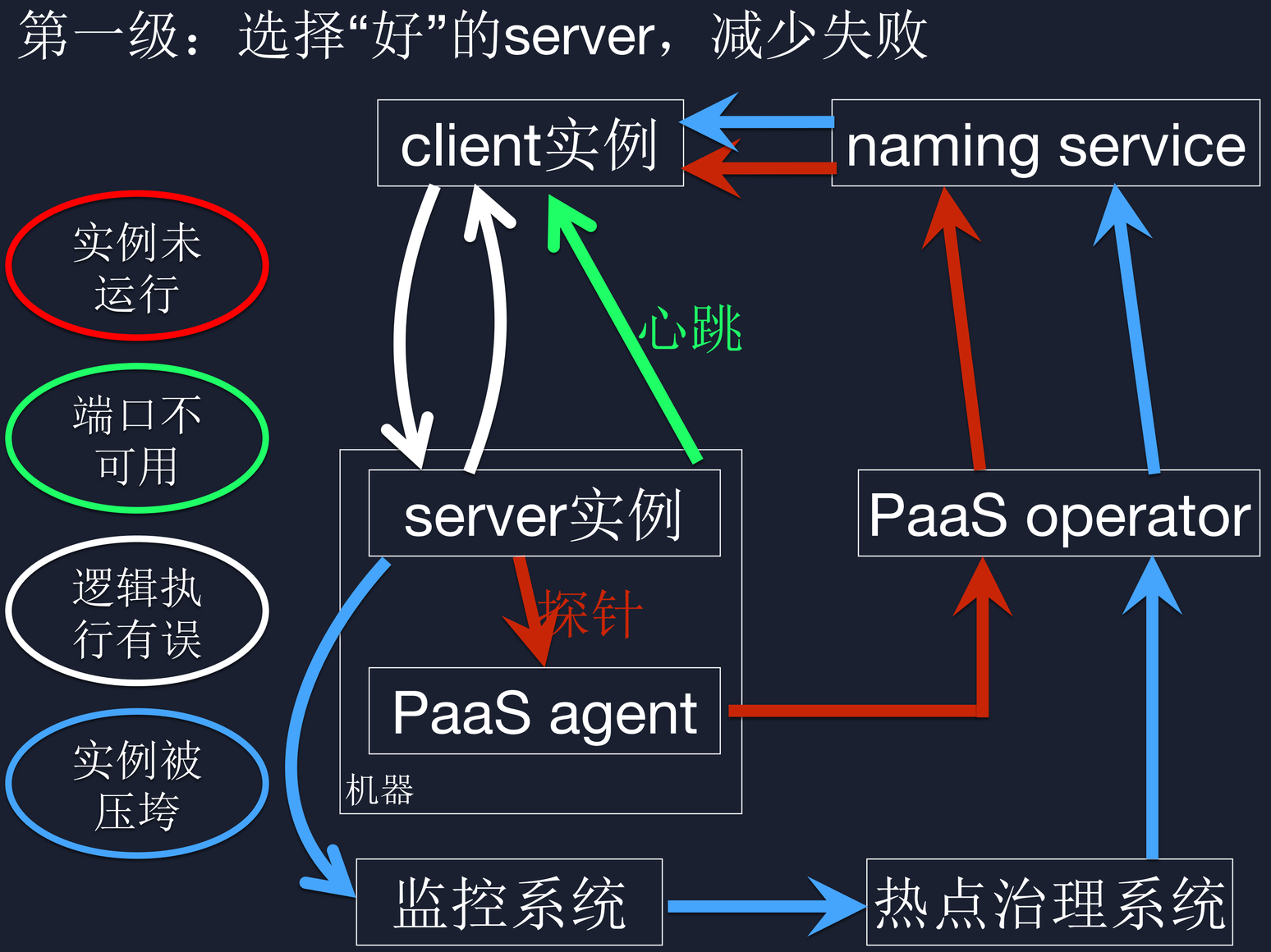


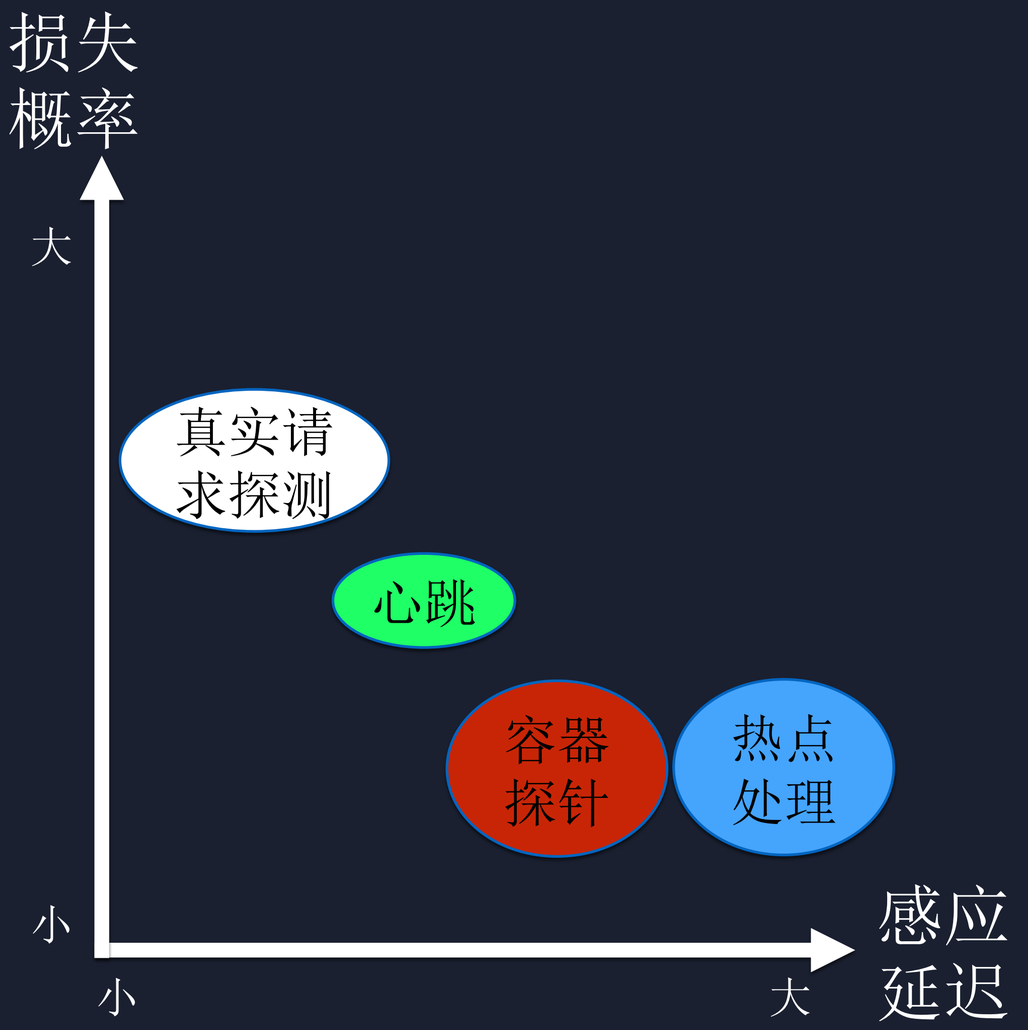
全面预防：流量调度框架



全面预防：流量调度框架|可用性感知

第一级：选择“好”的server，减少失败





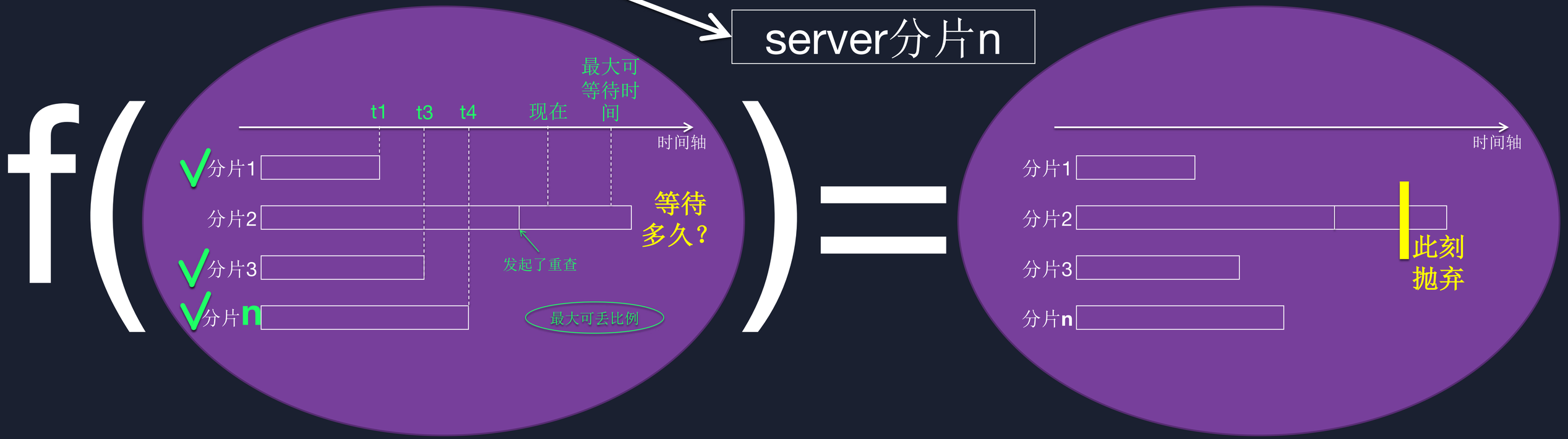
全面预防：流量调度框架|流量控制——分片场景

第二级：分片服务下，勇于“壮士断腕”，减少超时风险

query → client → server分片1 / server分片2 / server分片3 / server分片n

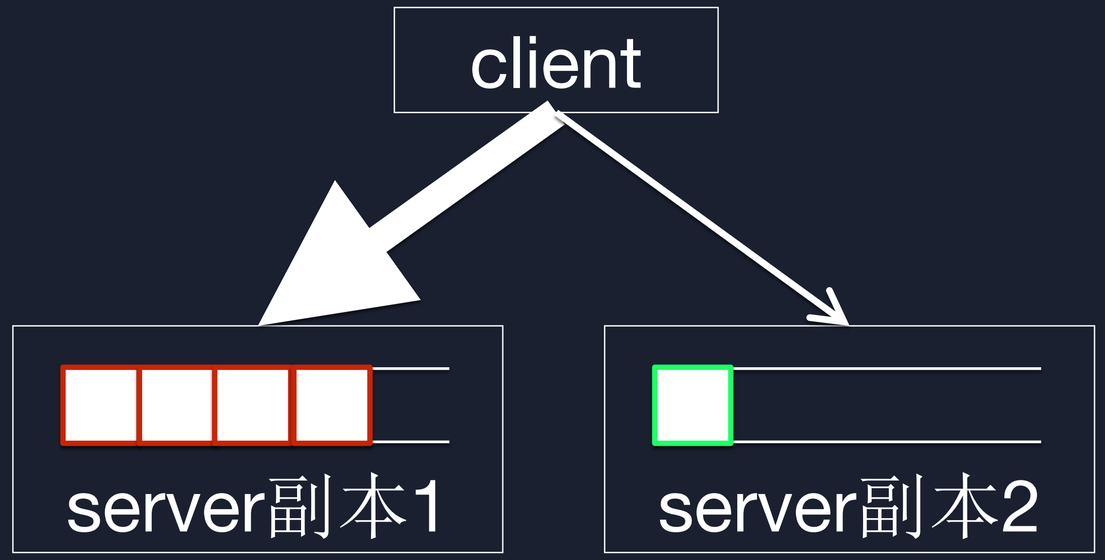
server反馈

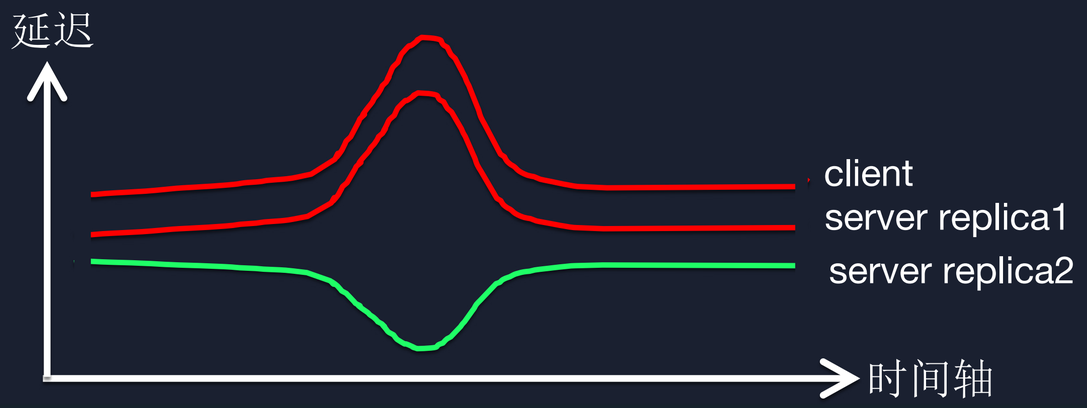
动态丢层



全面预防：流量调度框架|负载均衡——副本场景

第三级：多副本时，均衡化延迟，减少超时风险





算法	特性	使用场景
random	随机打散	server实例处理能力相同
round robin	依次调度	server实例处理能力相同
query word hash	按query内容哈希选取	请求具有聚集性，且server具备本地cache
静态weight	按权调度	server实例处理能力存在稳定的不同
动态weight（latency aware）	根据server延迟按权调度	server承载流量大，处理能力随时间变化
动态weight（cache aware）	使server副本本地cache数据产生差异，减少整体盘IO	server副本存在本地cache，query按更小的组成粒度访问这些cache
...	...	...

最佳实践

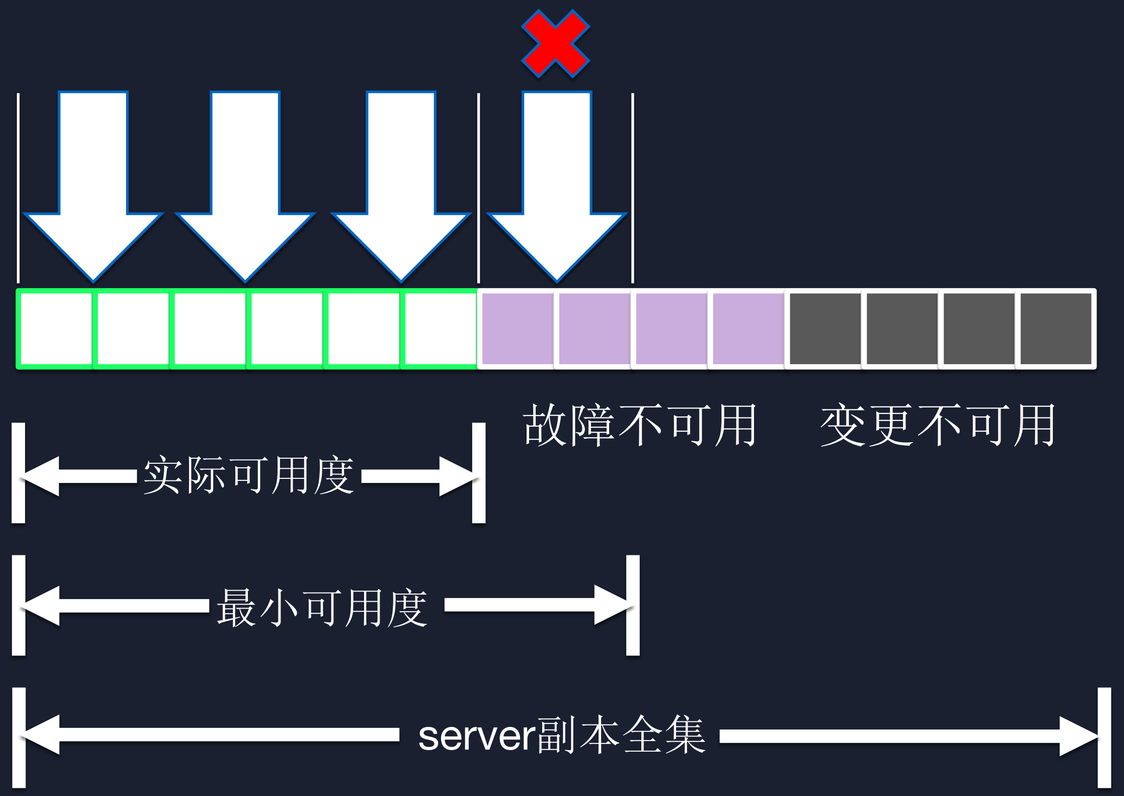
1. Random、RR
用全集群容量应对极端热词
结合外围机制杀热点

2. 动态weight
用于召回层：
大吞吐，少副本

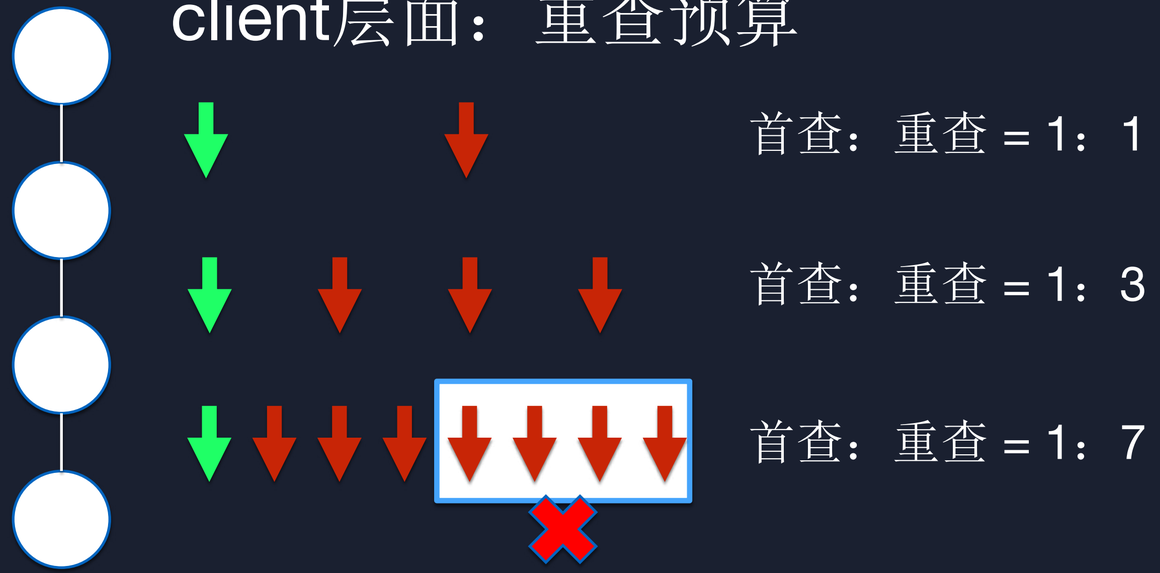
全面预防：流量调度框架|服务级别的保护

第四级：牺牲少数，保护多数，减少损失

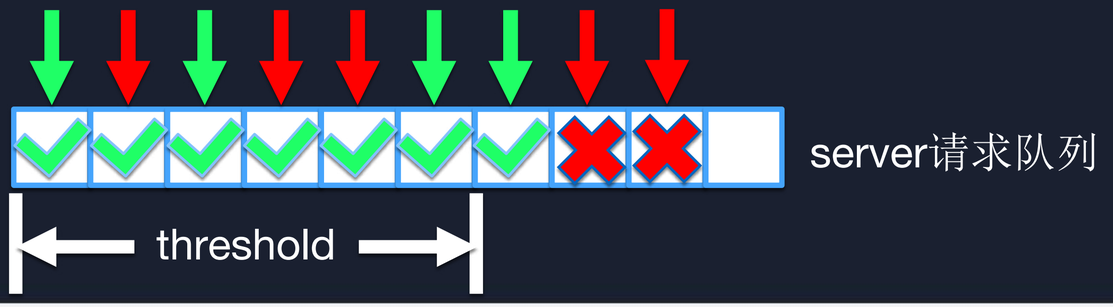
client层面：通过可用度保护server



client层面：重查预算

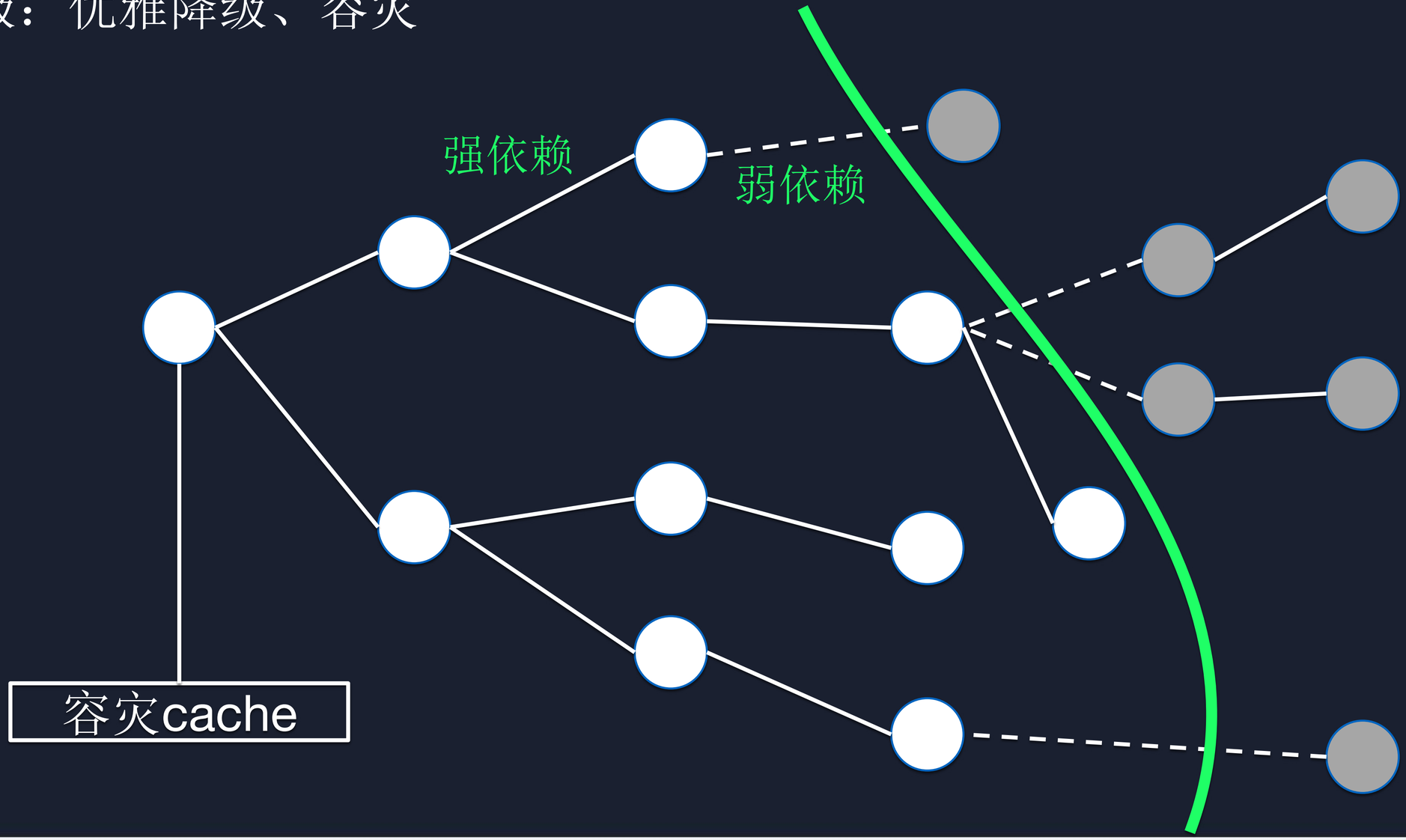


server层面：优先级限流

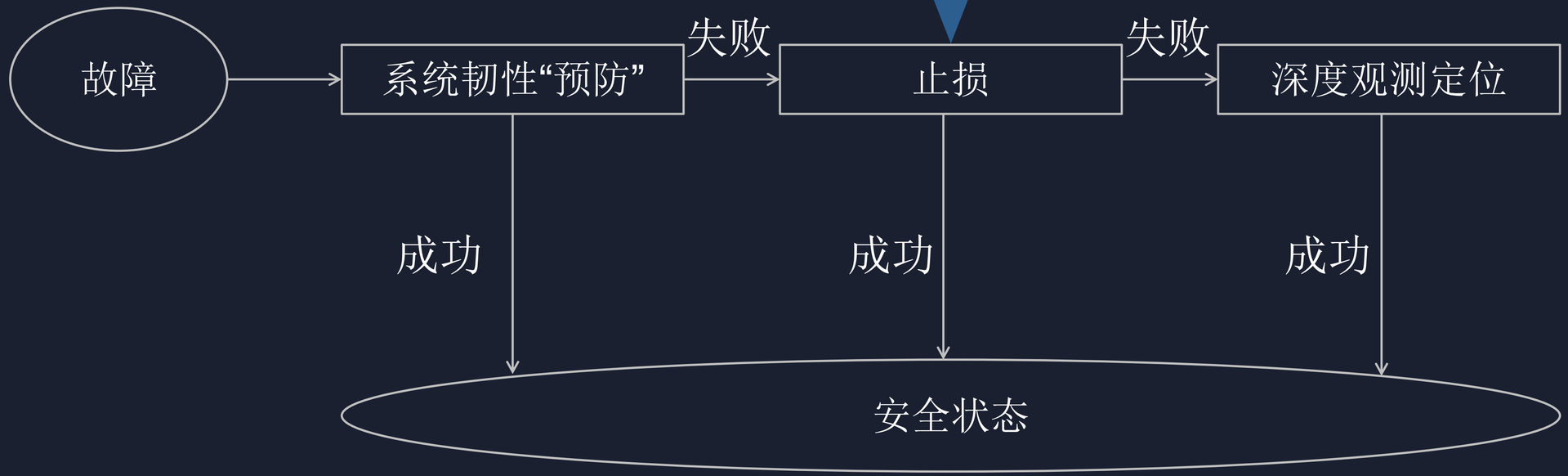


全面预防：流量调度框架|兜底

第五级：优雅降级、容灾



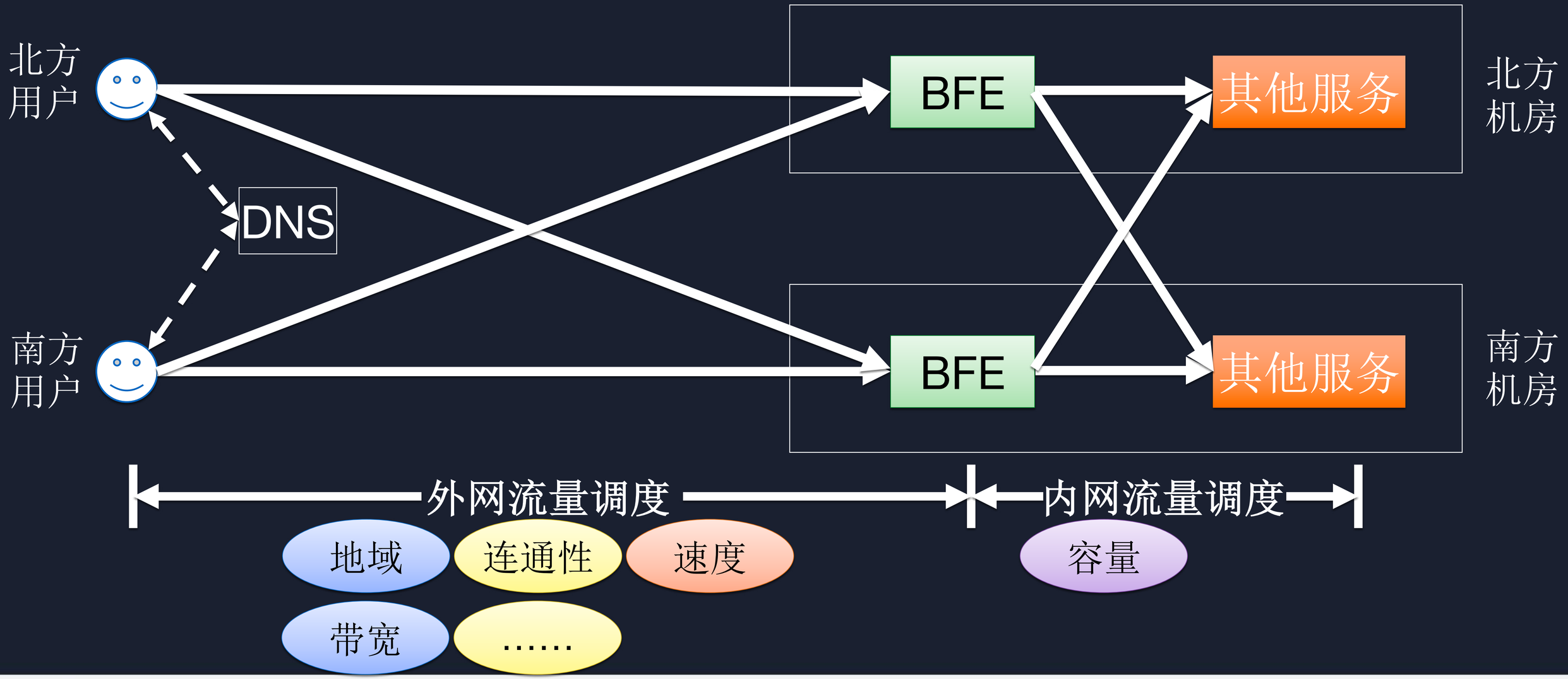
精细止损——流量切换、降级



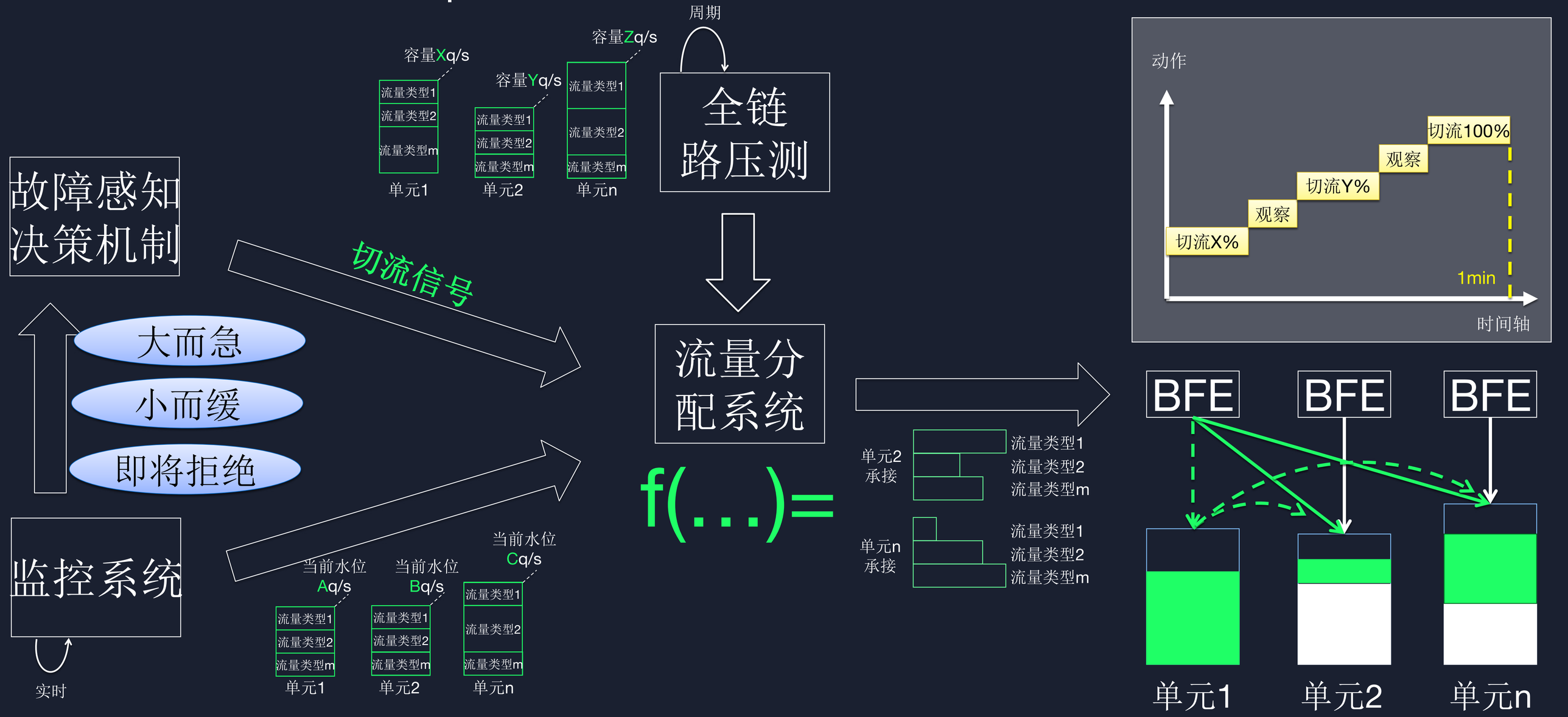
精细止损

目标：损失将要不可避免的发生、或者损失已产生，使损失最小。

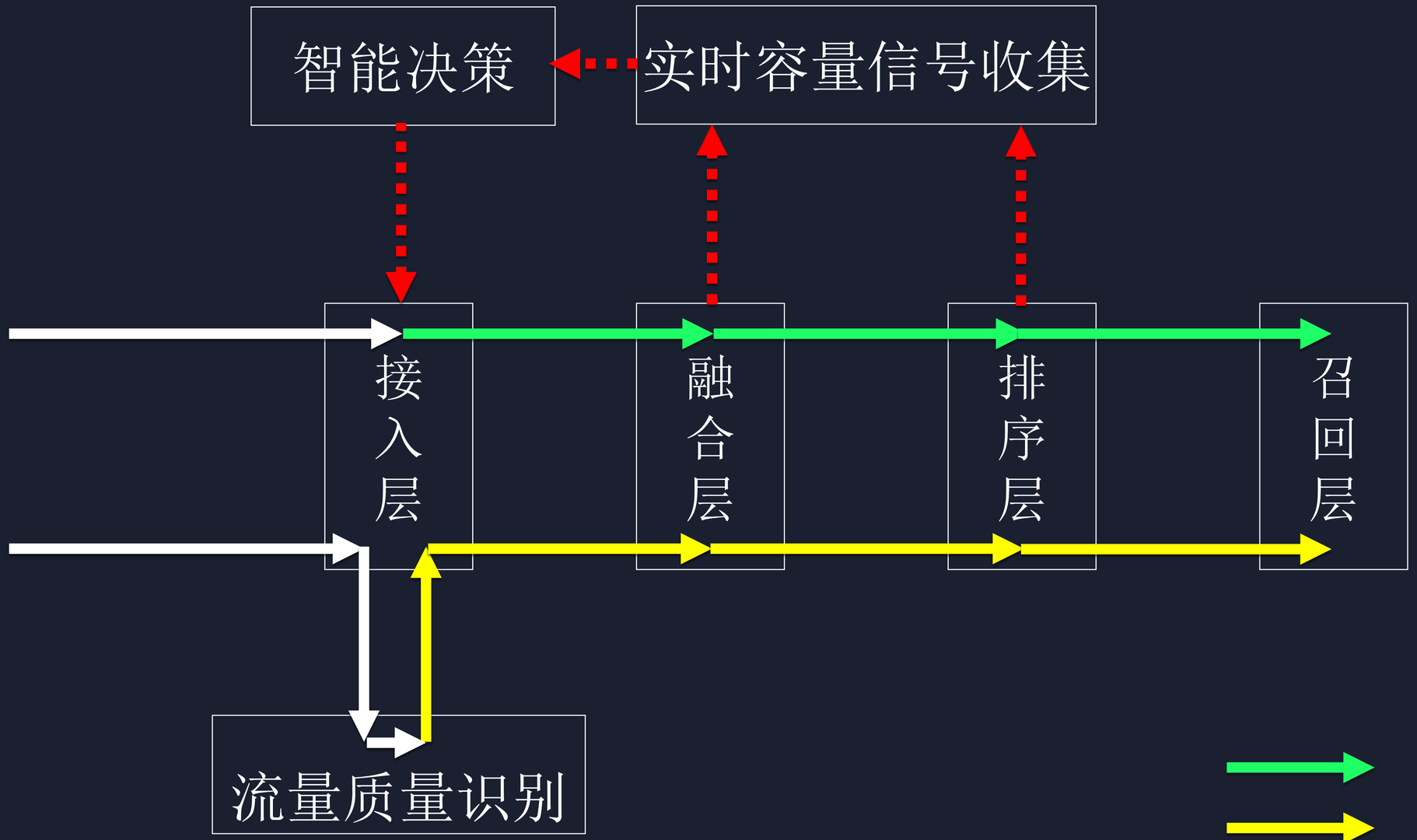
精细止损：流量切换|全局视图



精细止损：流量切换|内网流量调度



精细止损：降级|全自动降级



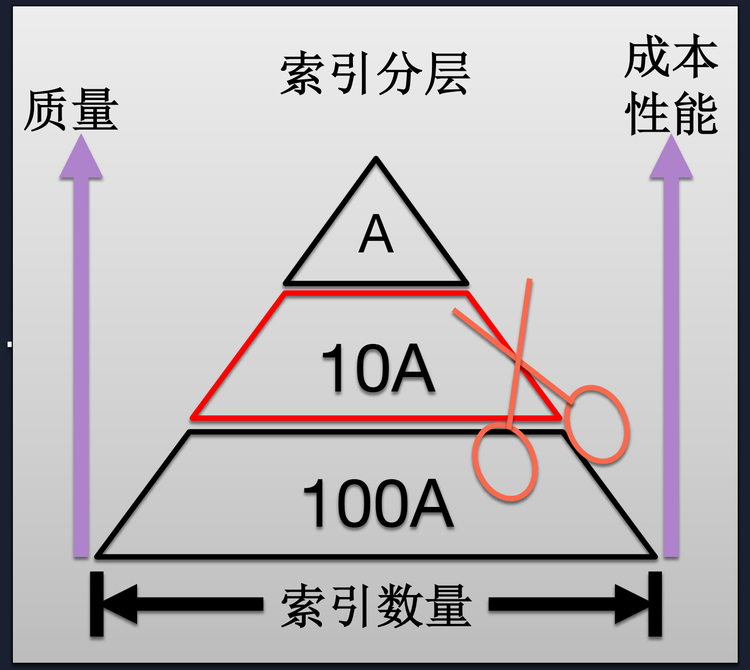
精细止损：降级|半自动降级手段和烈度

机器/人工决策

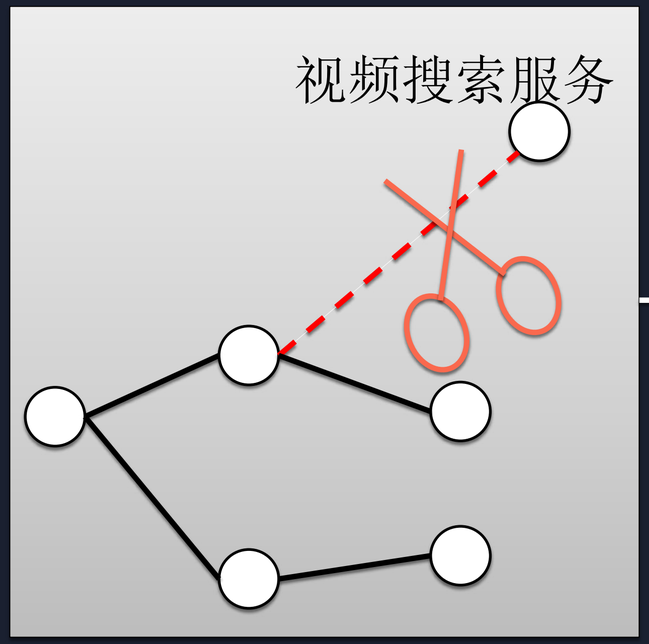
例如：
速度优化型流量

几乎
无影响

例如：
砍索引



视频搜索服务



例如：
摘服务

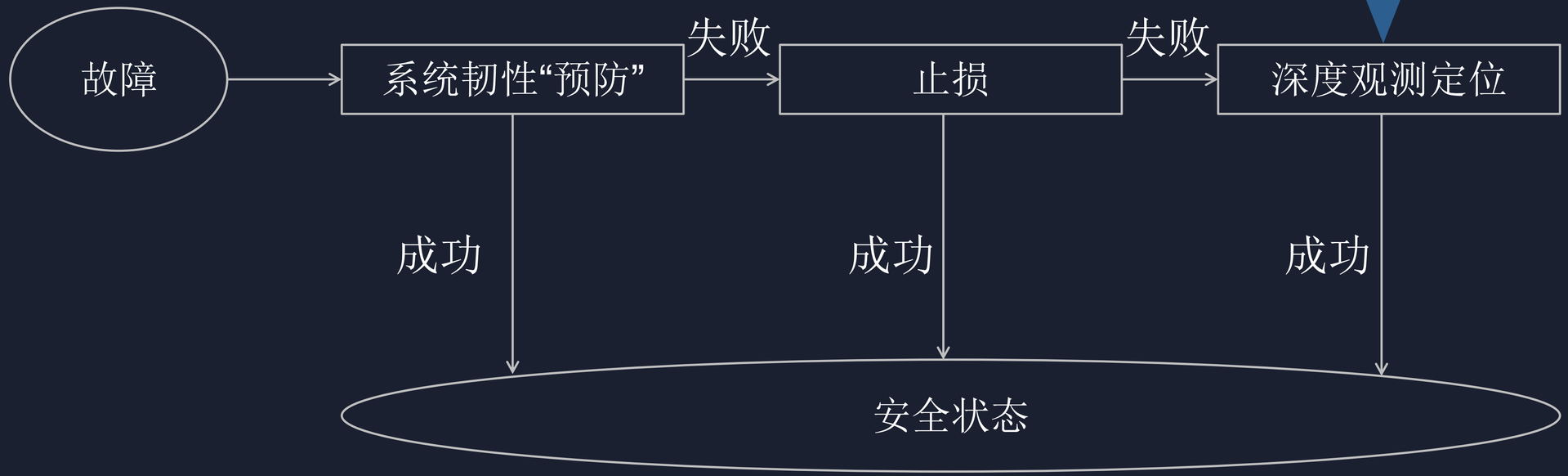
轻微影响结
果相关性

严重影响结果相关性
但仍无拒绝

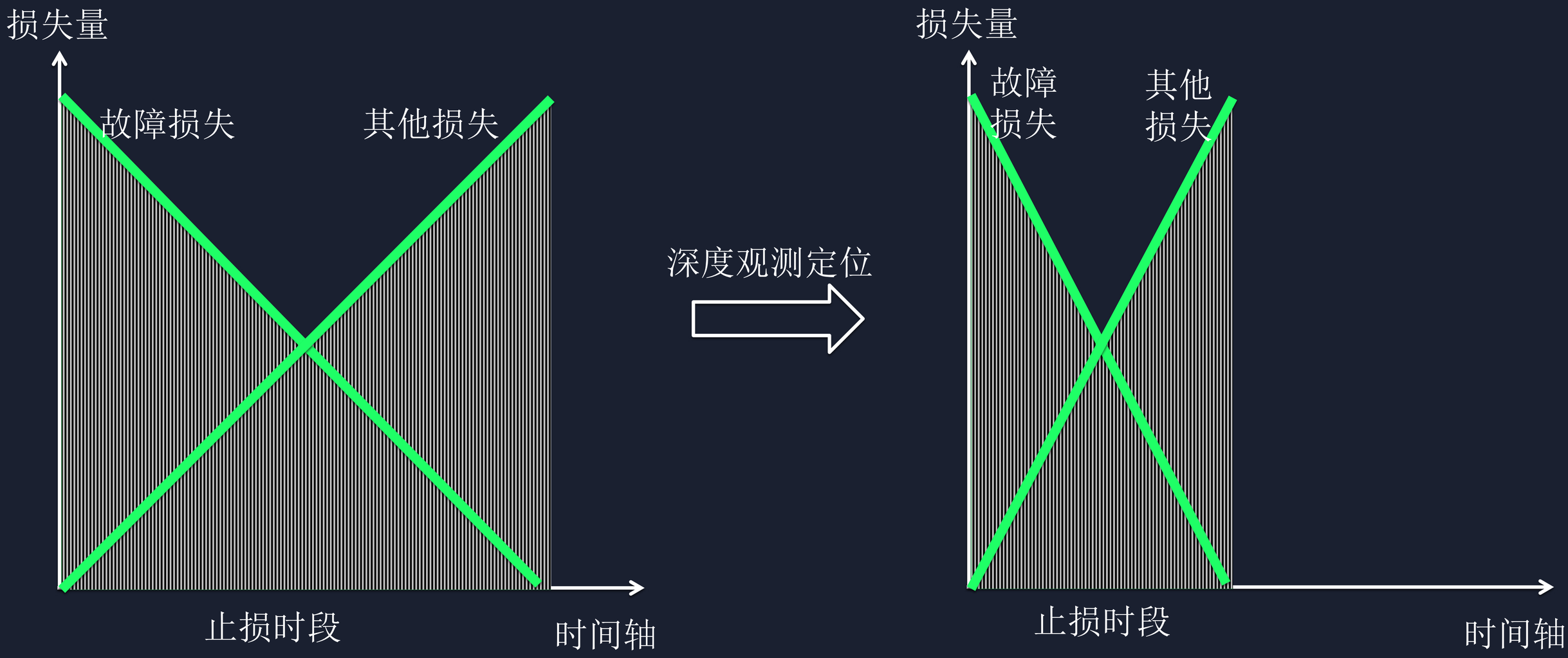
严重影响结果相关性
且伴随拒绝

例如：
接入层限流

深度观测——tracing、logging、自动分析



深度观测|追求

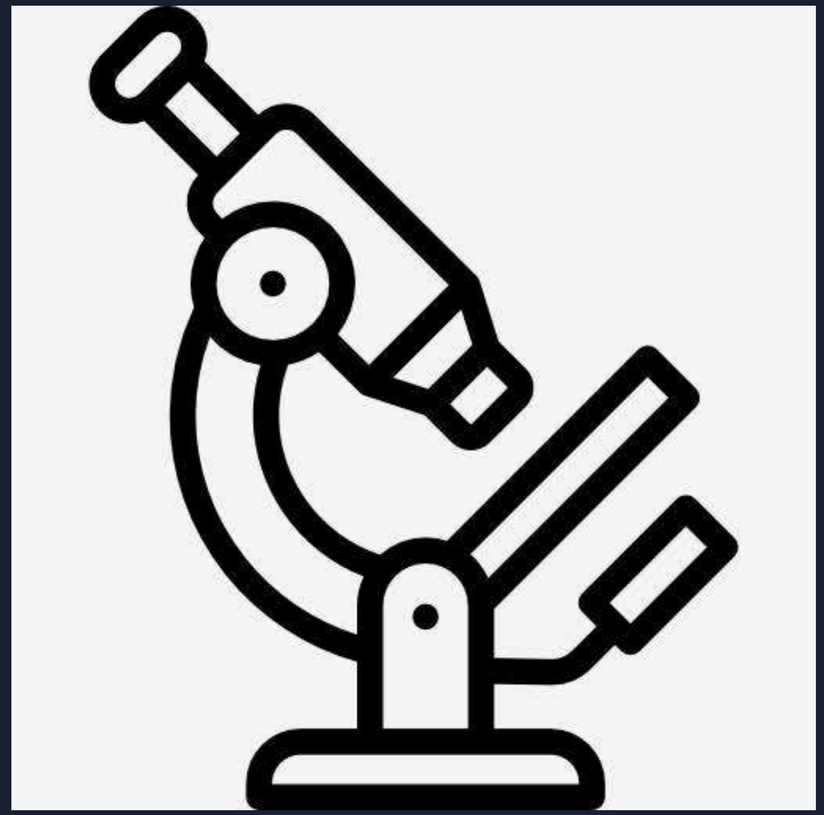


深度观测|场景

故障未发生：发现系统优化点

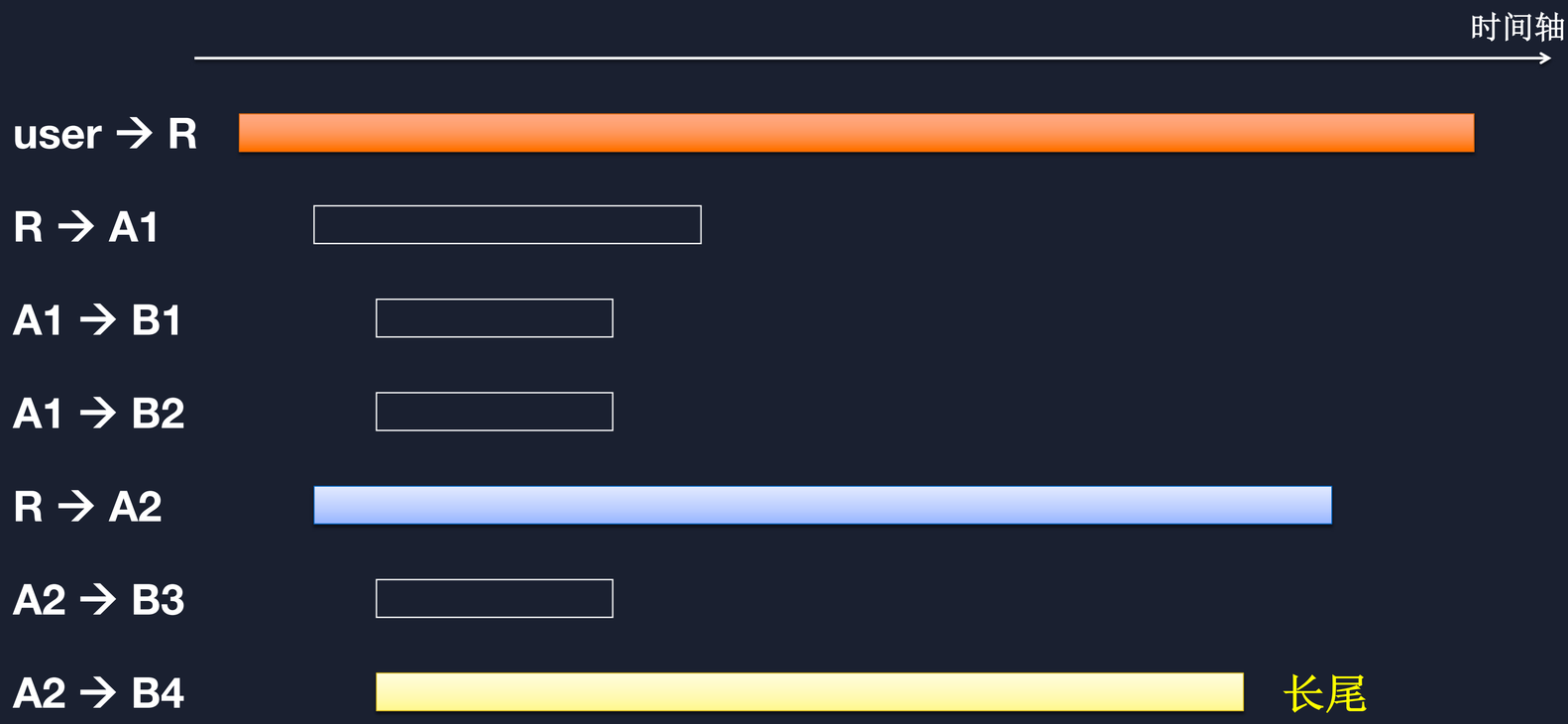
故障发生未止损：有效止损

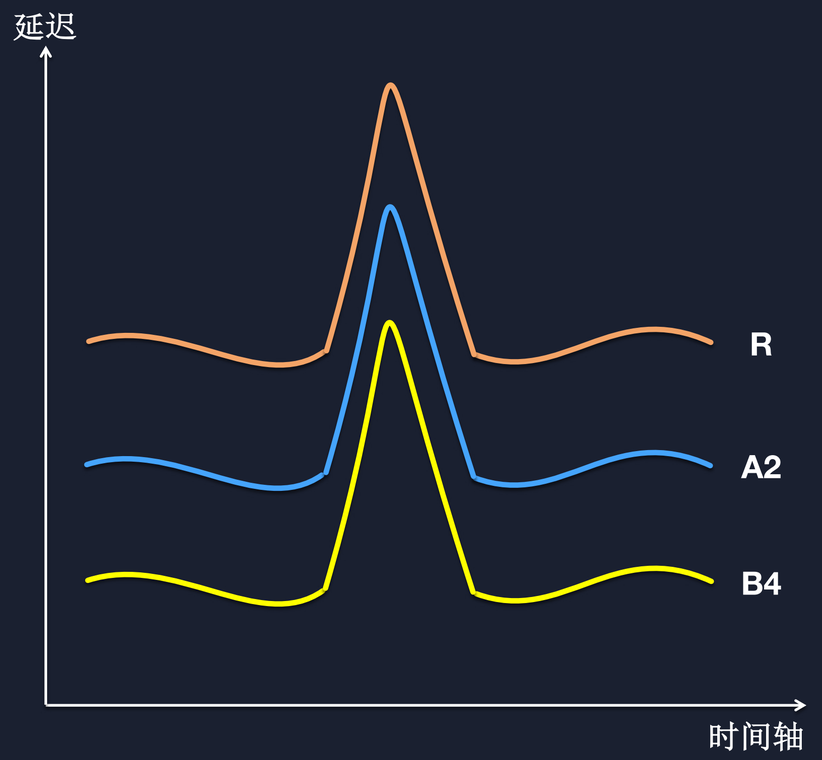
故障发生已止损：彻底消除缺陷



深度观测|其他问题形态

速度问题





问题现场

深度观测|需求

任意历史query的

- 节点信息
- 时序信息
- 日志信息

深度观测|可观测性发展历史

理论：dapper模型
抽样模式
调度链和annotation

引进来（2014）

- 一定程度白盒化
- 部分query得以分析
- 资源开销大
- 历史query无法全部分析

自研
全量时序
全量日志

创新（2016）

- 全量，数据建设彻底
- 任一query皆可分析
- 分析仍需人工参与

自研
自动化故障分析

再创新（2017）

- 全自动分析
- lowcode扩展
- 革新了工作模式，效率极大提升

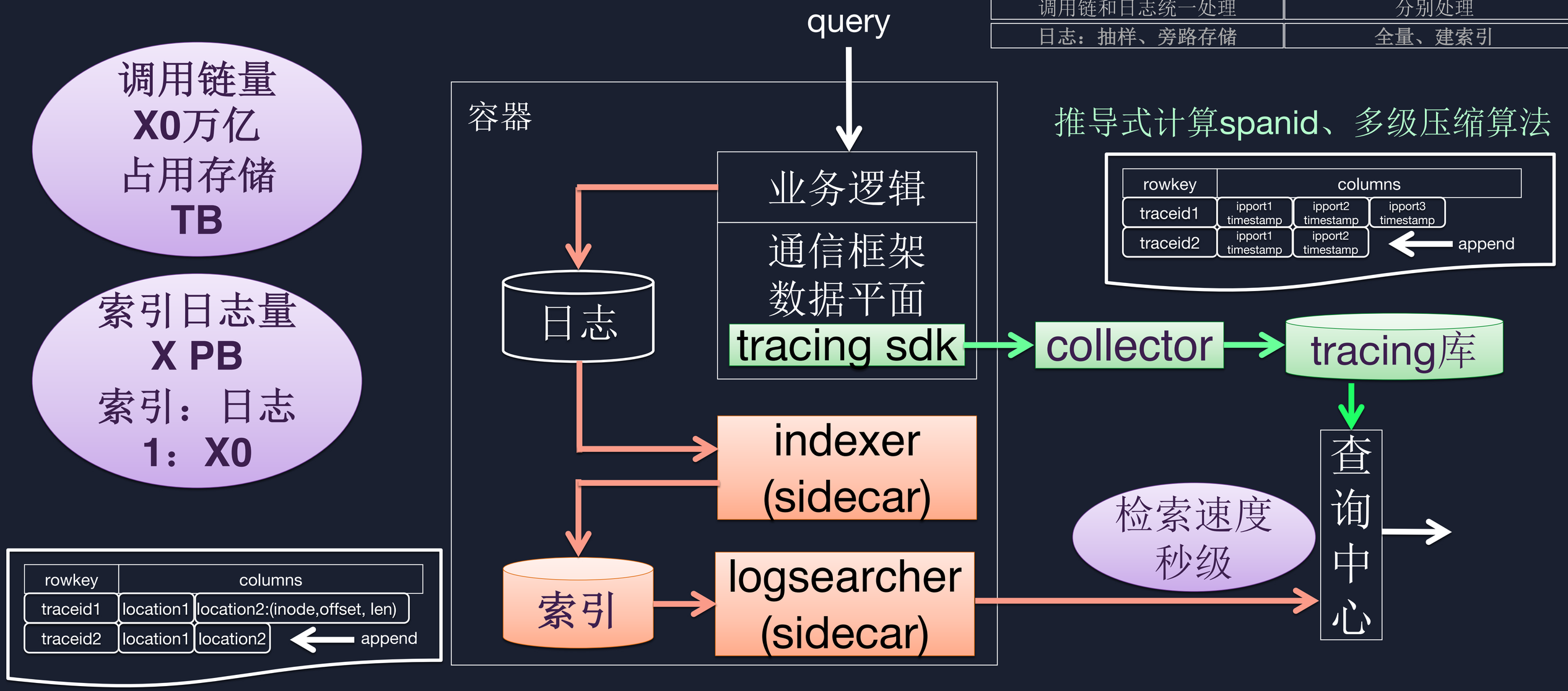
- pros
- cons

深度观测|全量调用链全量日志系统——kepler

类dapper系统	我们
调用链概念：traceid, spanid	相同
基于抽样	全量
存储：spanid入库	spanid推导计算、不存；多种压缩
调用链和日志统一处理	分别处理
日志：抽样、旁路存储	全量、建索引

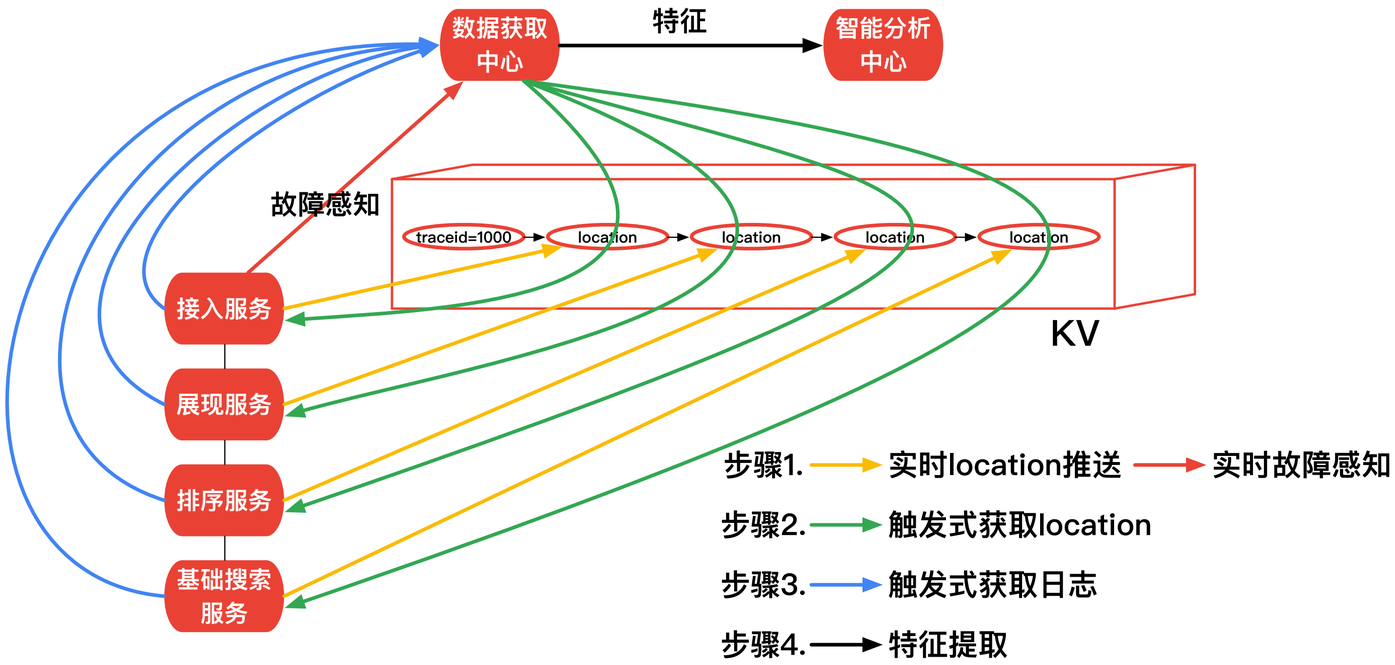
调用链量
X0万亿
占用存储
TB

索引日志量
X PB
索引：日志
1：X0



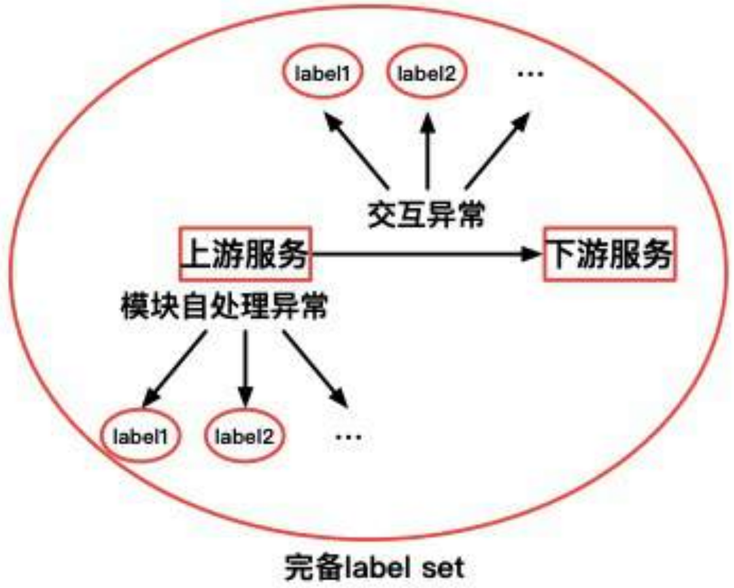
深度观测|拒绝自动分析系统——巨浪

通路



思考题：步骤1中的两条流是否需要有先后顺序?

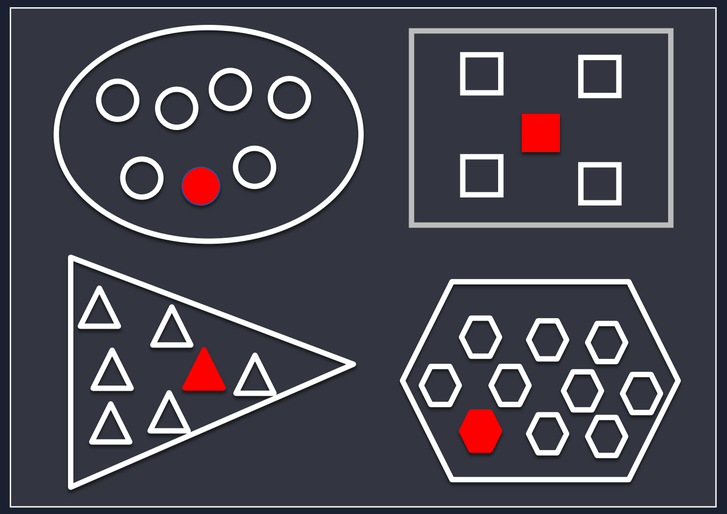
完备label set

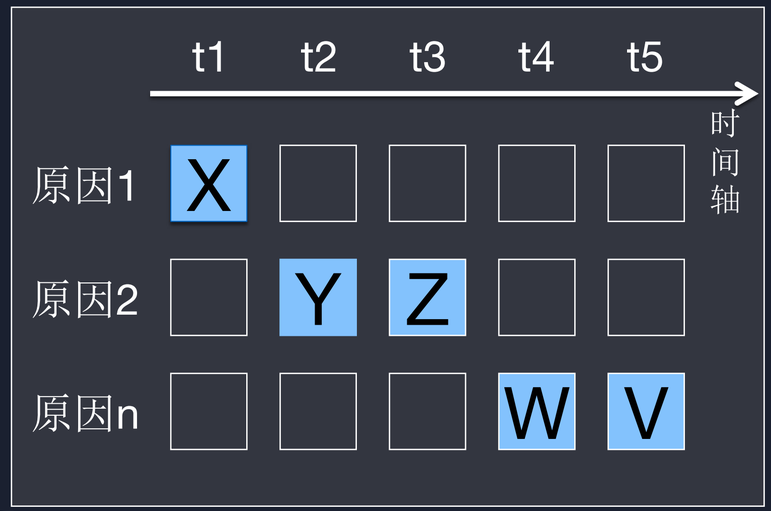


深度观测|拒绝自动分析系统——巨浪

特征工程

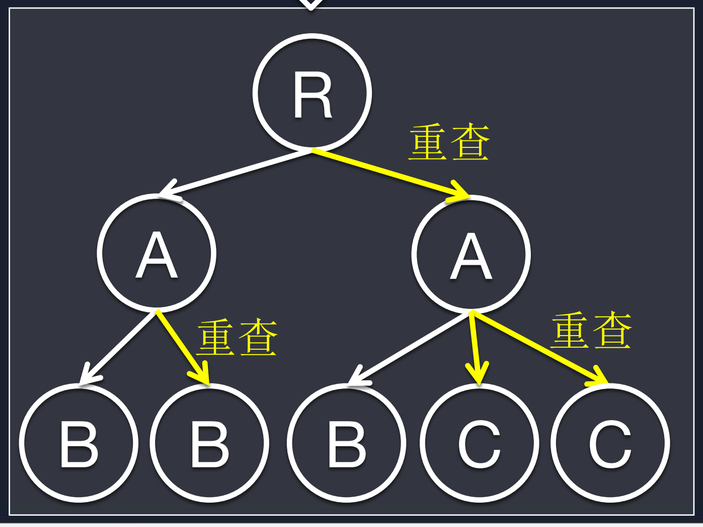
显著性分析





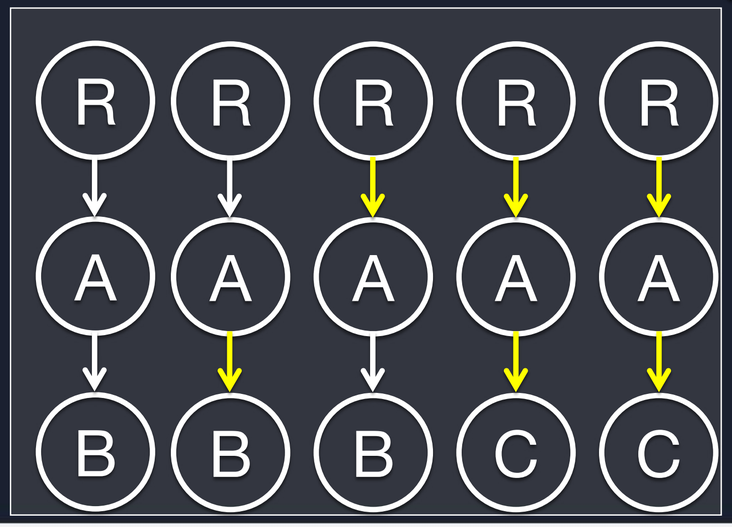
时间线还原

重查树还原

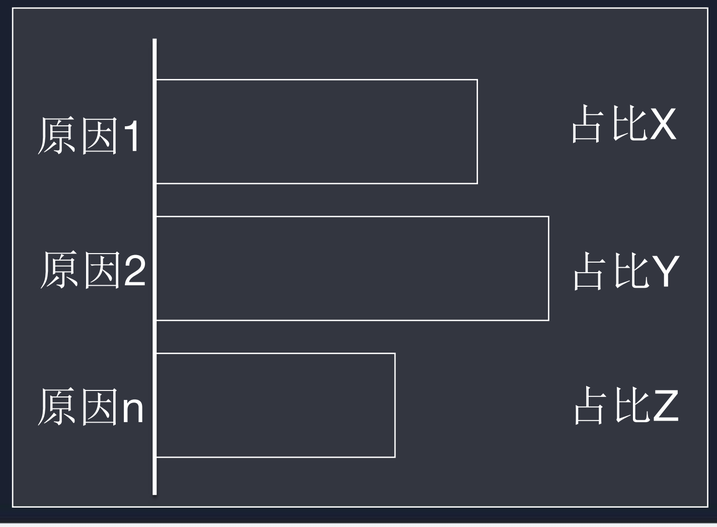


单故障
路径拆解

单路径
原因分析



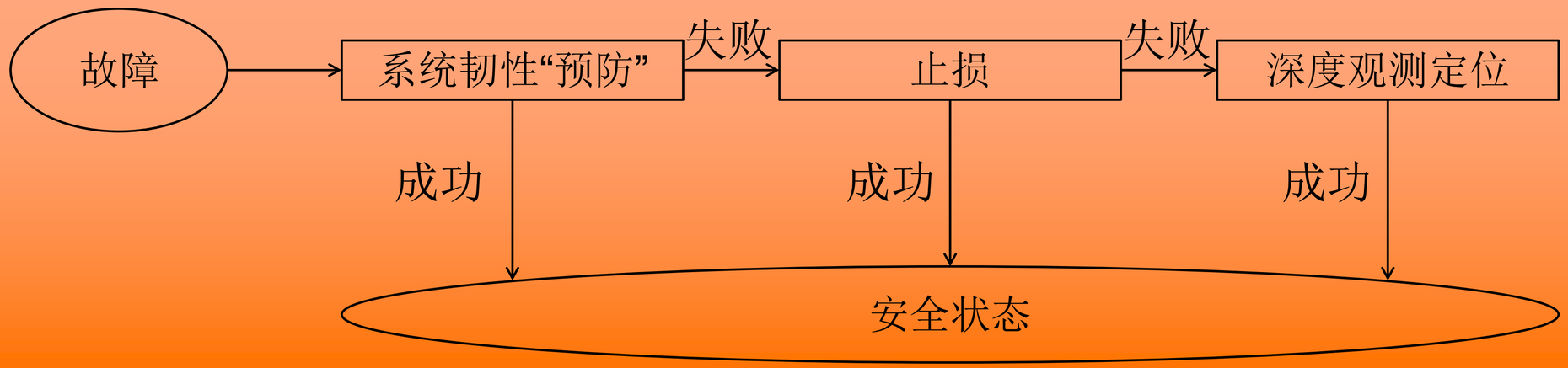
归纳



总结

目标：尽最大可能服务好query，减少损失

模式



全面预防

目标：提升系统韧性
组件之一：流量调度框架

多级治理手段：
1. 以小代价选择可用的server实例
2. 分片模式下动态丢层防延迟长尾
3. 副本模式下多种负载均衡防延迟长尾
4. 对server的多种保护使整体损失最小
5. 弱依赖容忍、强依赖容灾兜底

精细止损

目标：提供无脑但又相对精确、迅速的手段
相关机制：流量切换、降级

流量切换：精准感知、安全高效执行
降级：多种手段释放系统容量

深度观测

目标：根因快速定位
原则：
1. 正视数据需求，毫不妥协地进行数据建设，建设全量tracing和logging
2. 故障分析全自动化，形成“非智力型”过程，解放人力，提升效率

THANKS

InfoQ | 写作平台

InfoQ 写作平台是 InfoQ 开放给**开发者的高端技术社区**，创作者可以在这里**自由创作和发布内容**。

写作平台将为创作者提供**签约、培训、资金扶持**等一系列权益，助力作者成长为高精尖技术人才；同时也为企业提供**品牌、活动打造、内容传播**等服务，与伙伴一同成长。

扫码申请创作者

企业/个人均可申请

扫码进入写作平台

打开技术大门