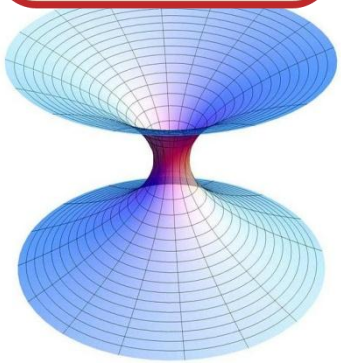


生产系统

快速恢复技术

——民生保险应用管理经理

杨春元

www.minshenglife.com

运维是什么？

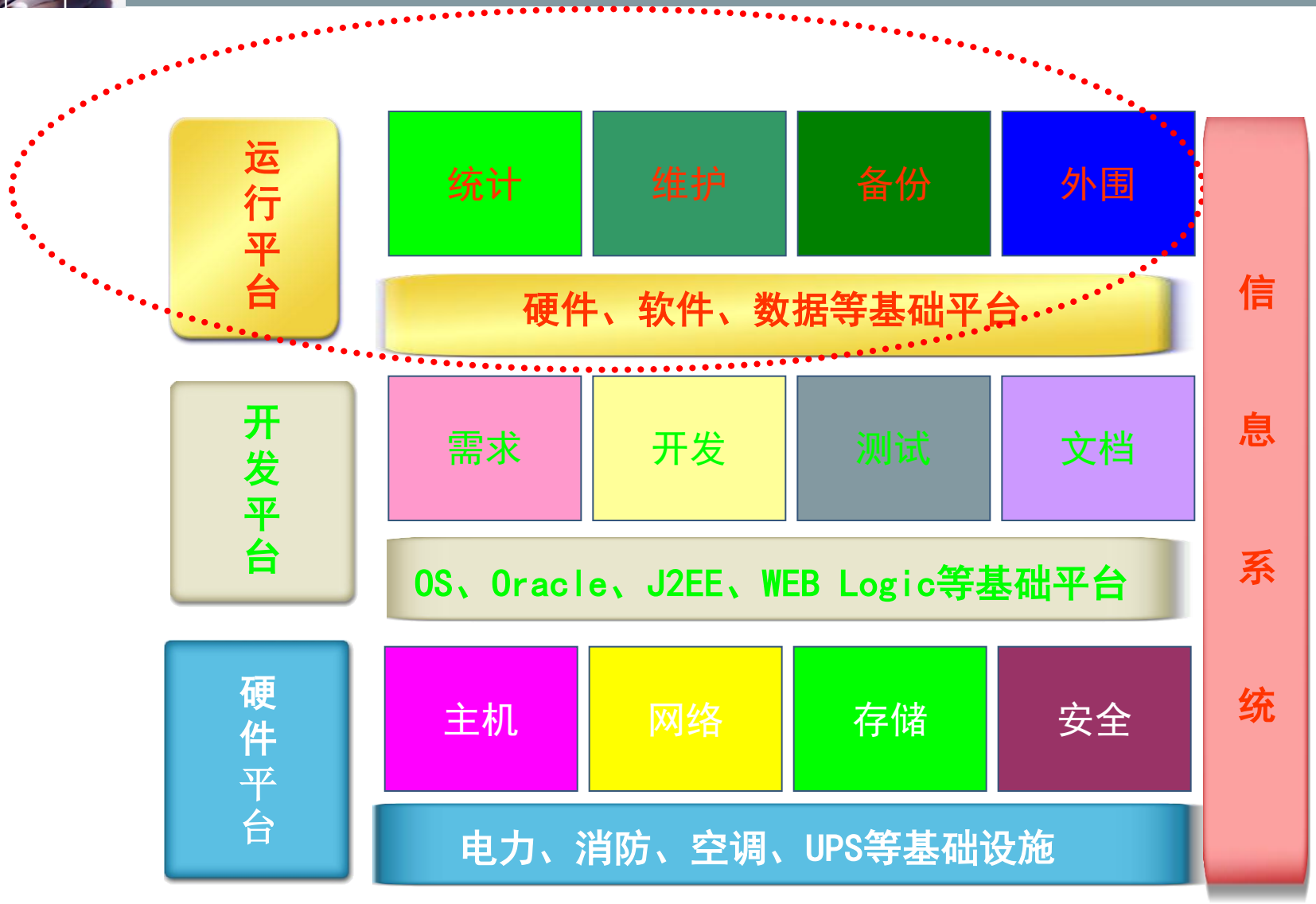
❖ 运维到底在做什么?什么样的运维才是好的？

- 系统运营是集基础架构、开发管理、业务处理乃至企业战略于一身的大事，系统运行的每时每刻都是战场。应用管理人员长期处于如履薄冰的状态，一方面微笑着服务，一方面随时警惕脚下的深渊。

运营人员的生活：

- 思考问题象哲学家、看问题象天文学家、定位故障象刑侦专家、思维严谨象逻辑学家、处理效率象数学家、博采众长象历史学家、措辞谨慎象外交家、文字功底象文学家。把最复杂的事情用最简单的话说清楚，则完全是一名早教家！

运维的定位



运维的内容

- **正常运行维护**

维护、事件、变更、上线、退役、备份、优化、预案准备
考核值班：故障率、故障次数

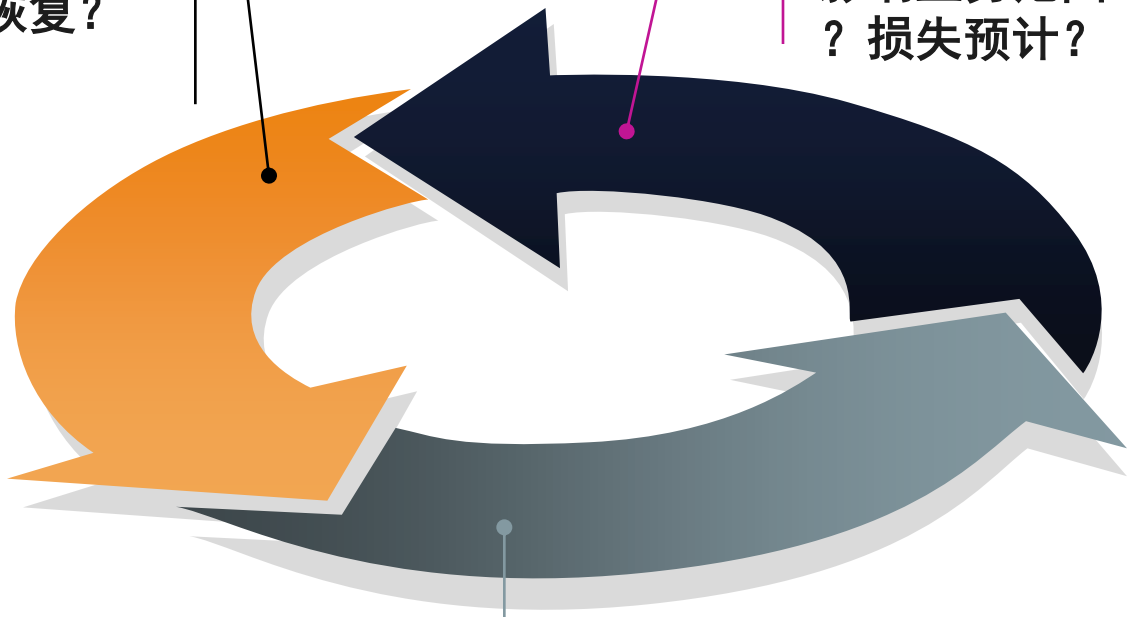
- **故障处理**

恢复生产、查找原因、信息披露
考核指标：RTO与RPO

故障发现与解决的一般规律

故障发现：如何发现？谁发现了（监控/用户）？影响业务范围？时间范围？损失预计？

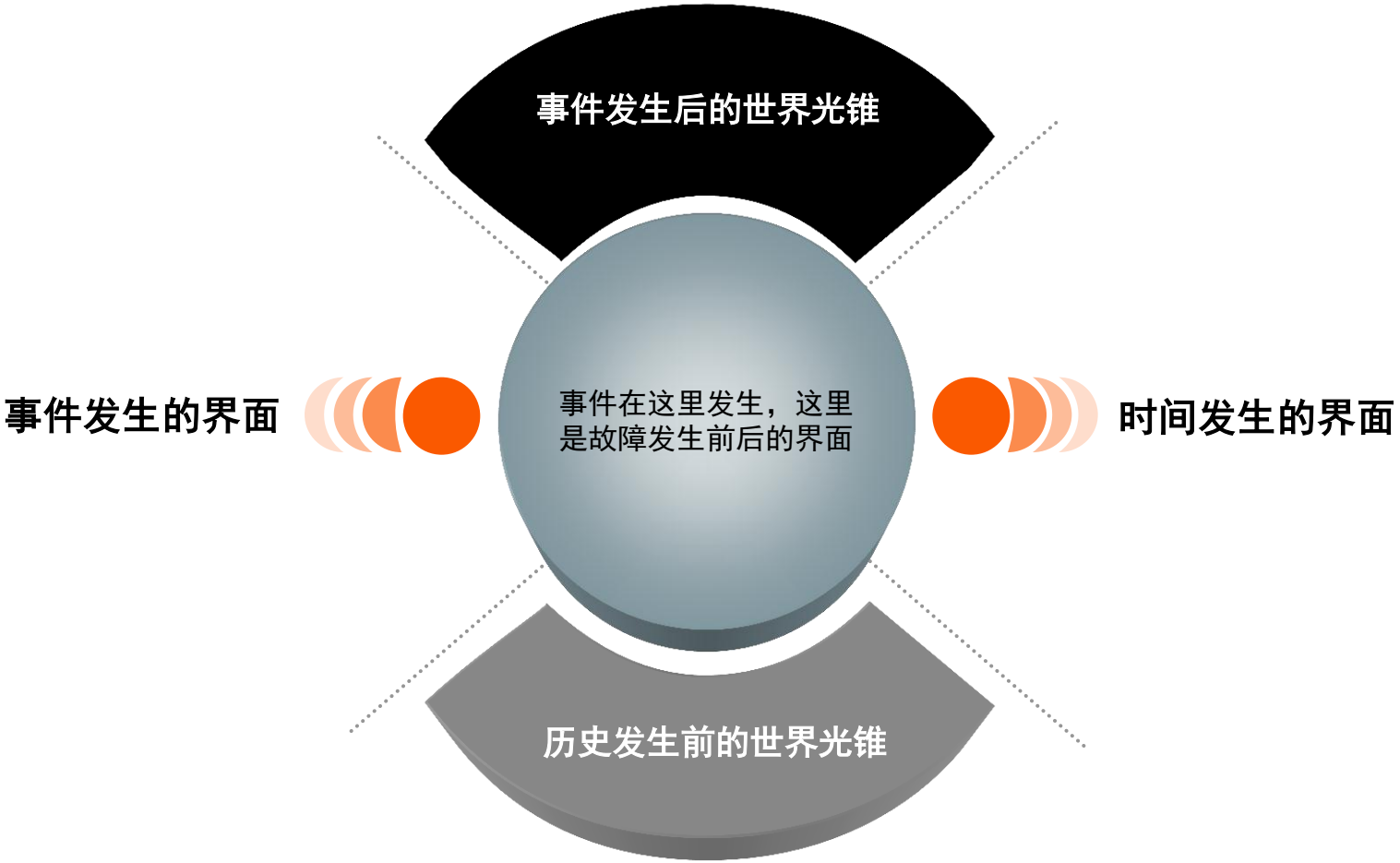
故障恢复：能不能恢复？如何恢复？最快恢复？



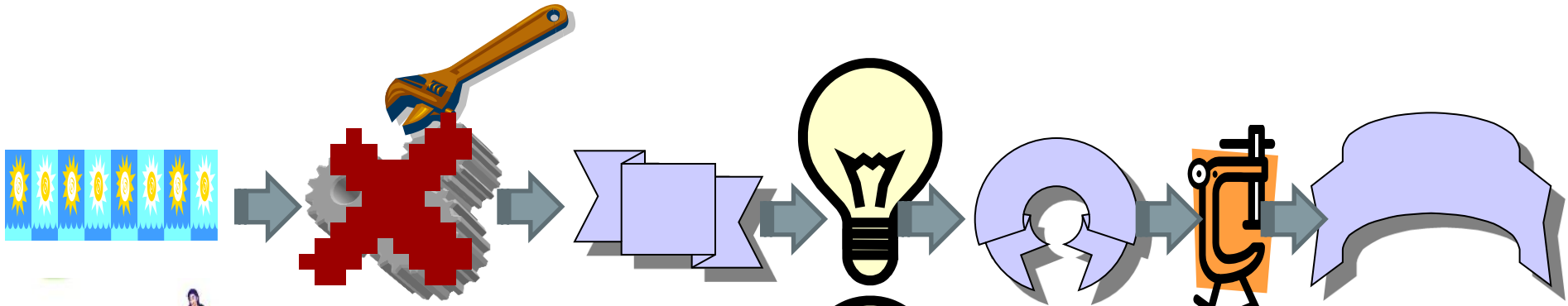
复盘：持续性改进措施？规避风险？转嫁风险？

时间简史

事件与时间


事件发生后的世界光锥
事件发生的界面
事件在这里发生，这里
是故障发生前后的界面
时间发生的界面
历史发生前的世界光锥

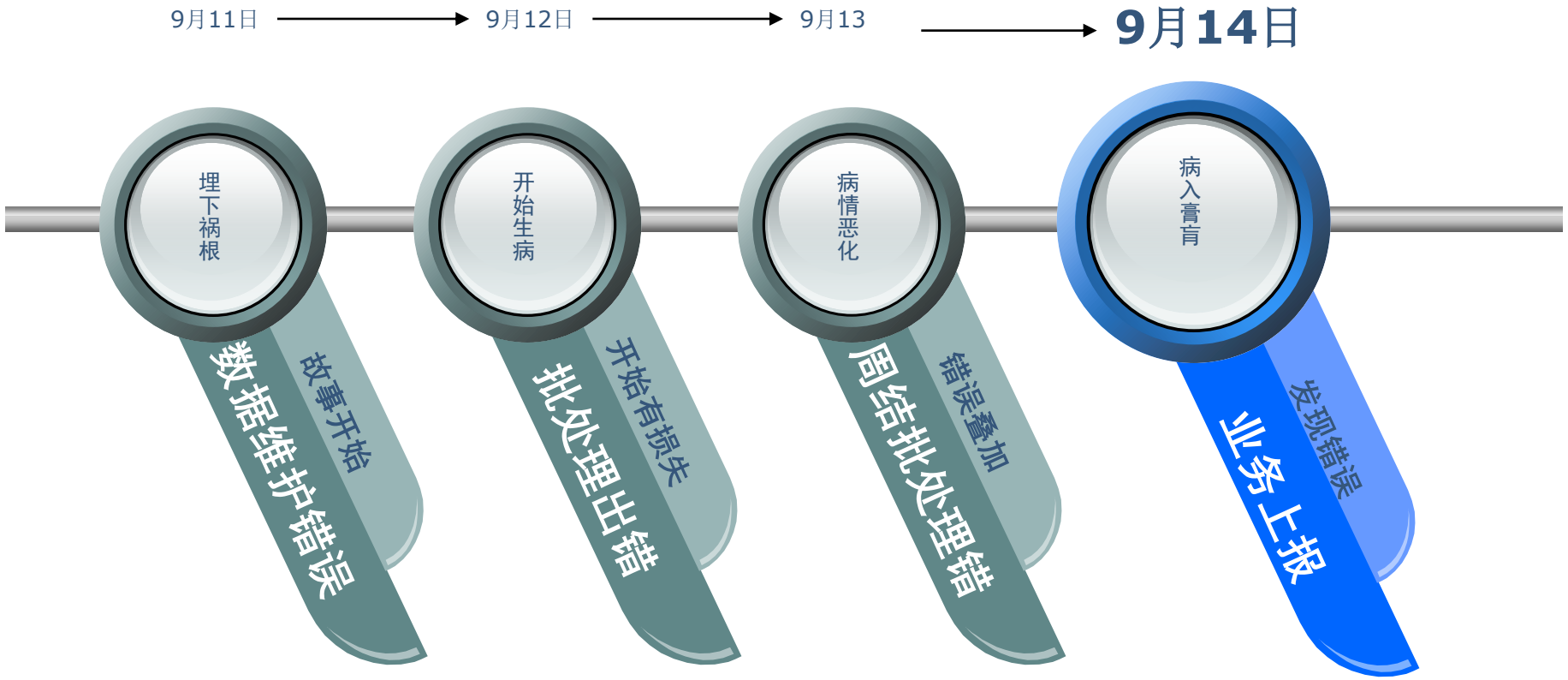
事件发生已经多日，还有希望还原吗？



事件发生已经多日，现场全破坏了，还能再现不？

- 某只软体动物出现了意外，于是人类就不会出现了——所以我们必需要拯救全人类。

一个批处理作业错误的例子



生产恢复的两大核心问题

能否恢复

是在正式恢复前首先要判别的基本内容。

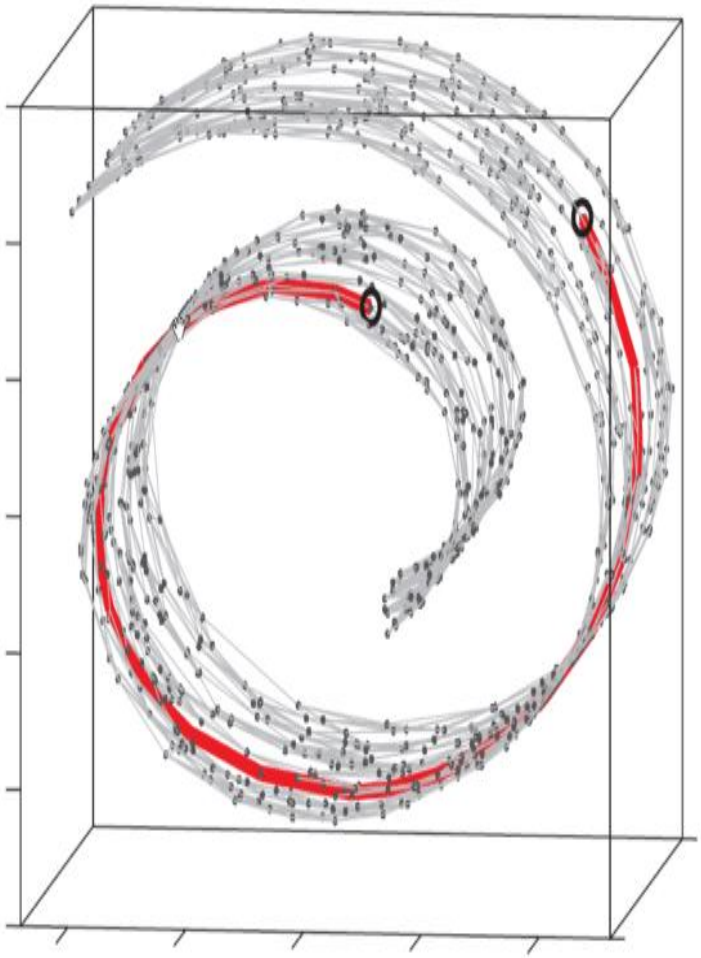
如何恢复

NRO、RTO、RPO是恢复的核心问题。有时候甚至是对用户影响最小的忙里偷闲恢复。

①可恢复时要恢复；

②不可恢复时要重构。

可恢复性必要条件的判定



$$A \circ G \circ G^{-1} \equiv A$$

- 一一映射且工程上可逆
  - × 大数分解
  - × 离散对数
  - × 哈希函数
  - × 浮点高精度计算
- 留痕
  - × 有路标的单行线
- 结果集范围容易确定
  - × 一只黑色公羊和一只白色母羊都变成了白色公羊，且被赶到了一群白色公羊里面

可恢复情况下如何恢复

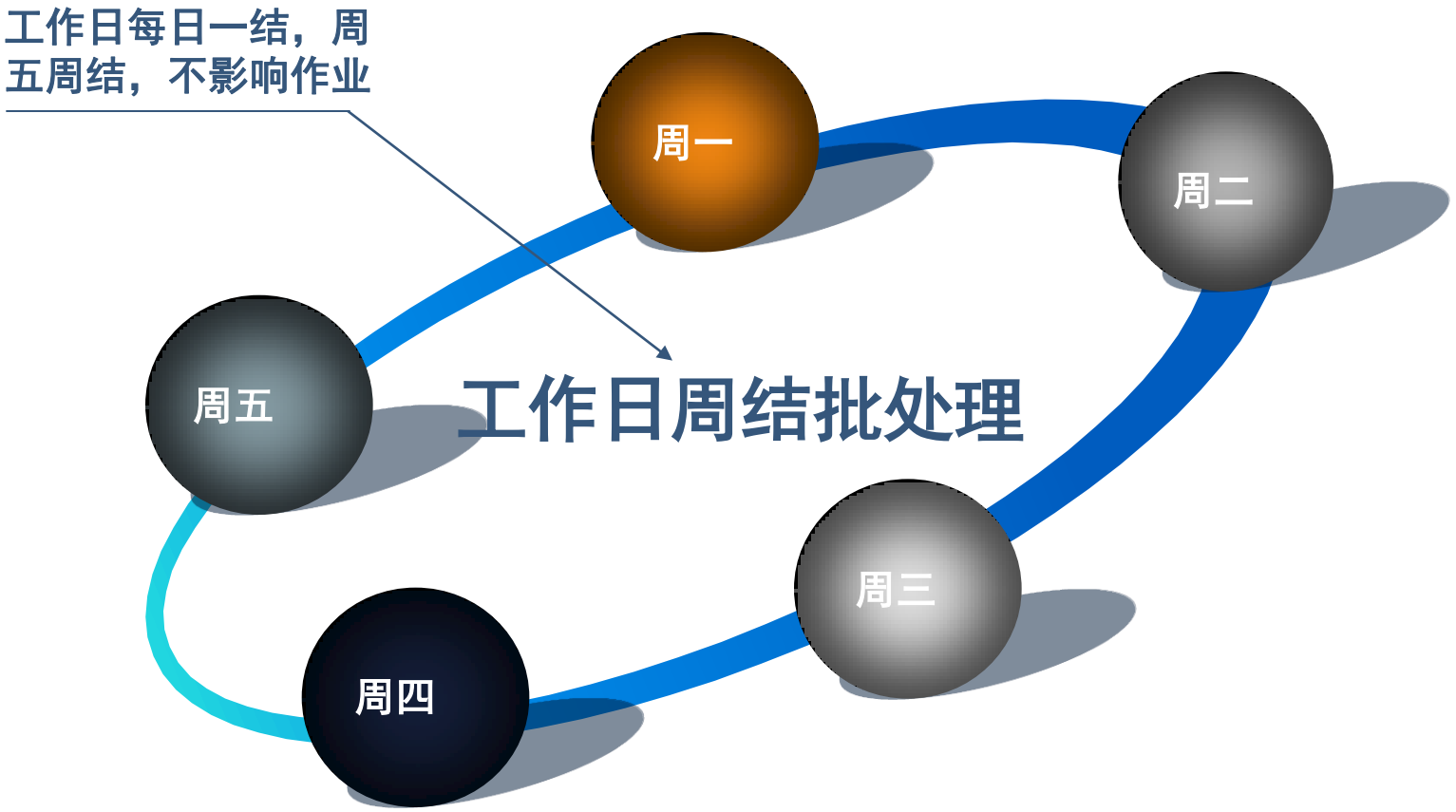
（一）忙里偷闲式恢复

- 局部功能暂停
- 特定范围数据不用
- 故障部件逐步替换(在线搬迁时可借鉴，尤其是采用负载均衡器+中间件的模式时)

（二）快速恢复

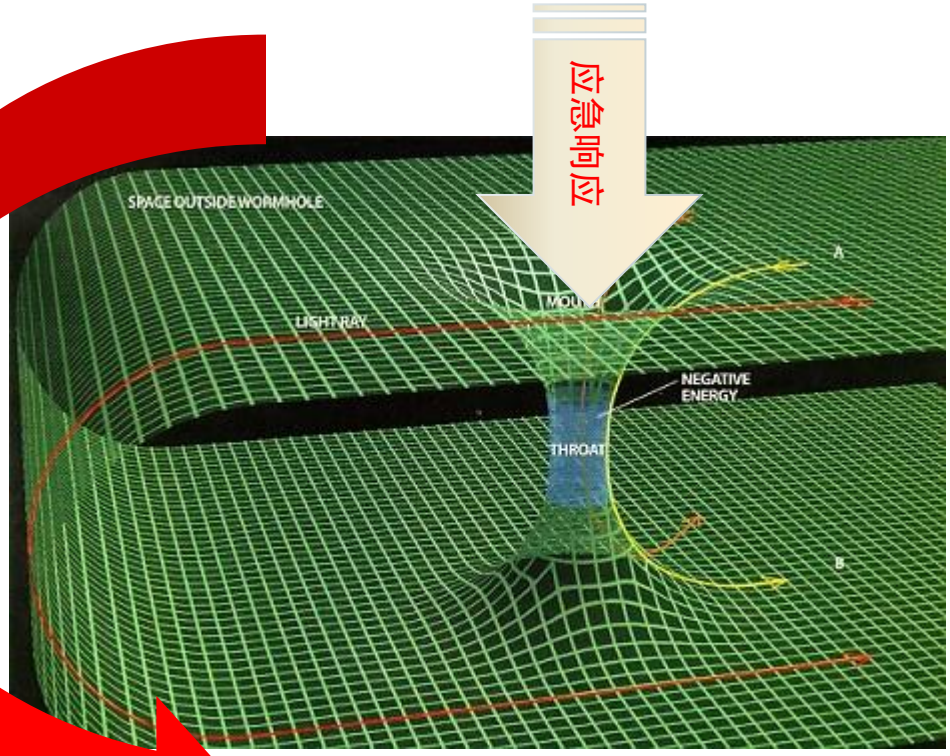
- 裁弯取直（虫洞）
- 并行

裁弯取直的典型案例——批处理

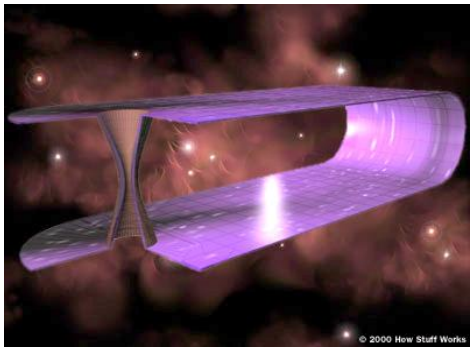


虫洞模型

正常批处理过程

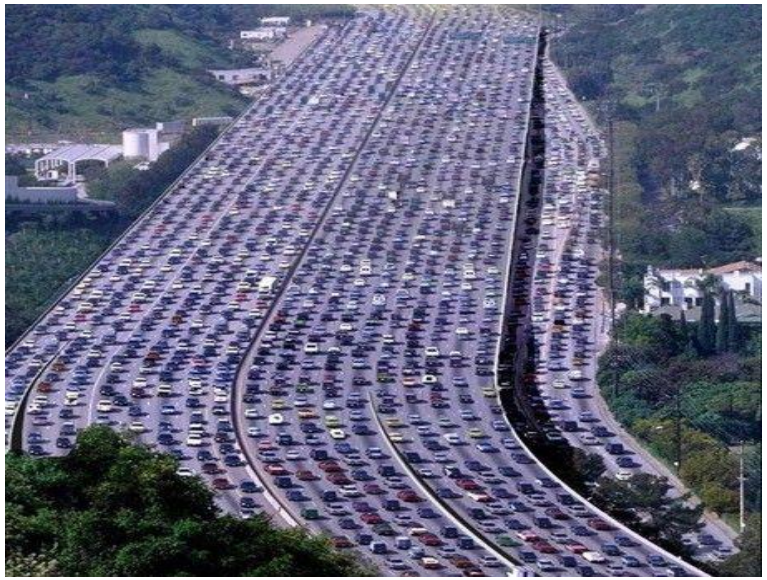


- 报表类
- 批处理类
- 数据订正



快速——并行思想的应用

①单任务
不能充分利用系统资源。



②适度并行
在生产模式下的首选方式。

③过度并行
大多数情况下不适合于生产，但是个别时候可以用于故障恢复。类似于抢险救灾，最大化利用承载能力。

并行执行的一般原则

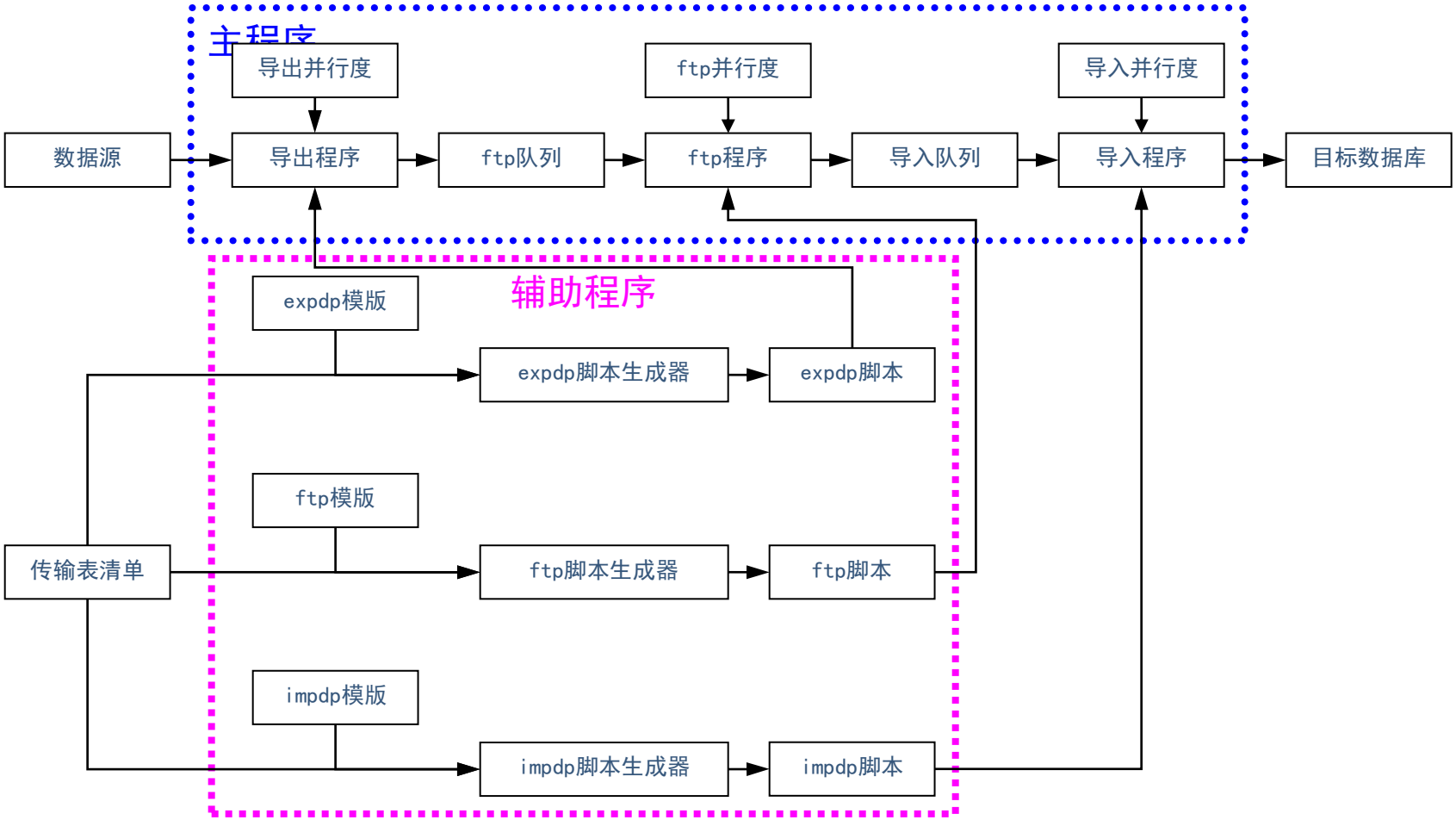
根据任务分层、大任务优先、所有资源充分三个原则执行。

- 如果任务有多个步骤，就要划分为多个层次
- 同一个层次的任务是可以并行的
- 不同层次的任务必需串行，且有严格的执行顺序

- 如果可同时执行的任务数量少于要执行的任务数量，那么优先执行大任务
- 按照每个任务执行所需的时间从大到小排序执行
- 当前任务执行完毕后，执行剩余任务中最大的任务

- 在多个层次的情况下，要确保总体上资源空闲越少越好
- 每个局部都最优不保证全局最优，适当取舍可能更佳
- 大多数时候想做到全局最优是困难的，次优方案也许是最佳选择(混沌学)

多层次并行的实例——三层（跨库复制）



2009年14分钟600GB oracle数据库9i→10g

不可恢复情况下的数据重构——技术原理

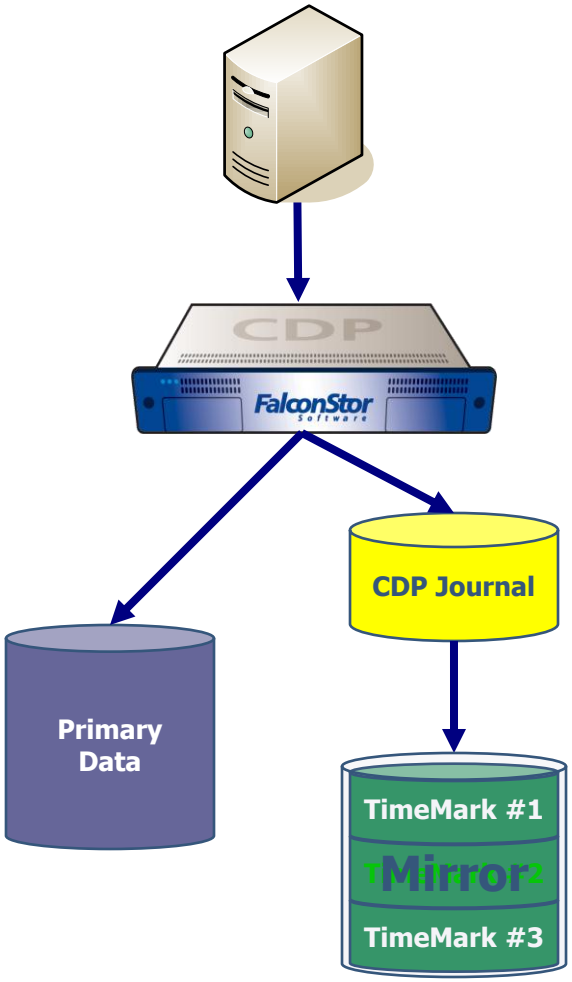
由于某种原因，不可能完全恢复，只能恢复到业务状态的某一特定时点，然后严格按照原系统的输入条件进行推进。适用范围：

- 基表业务数据受损；
- 发生不可逆的操作错误；
- 重构的成本远低于恢复成本：报表类系统、批处理补提

数据库RECOVER；
备份系统恢复；
CDP：飞康或EMC存储设备提供；
…… ……

不可恢复情况下的数据重构——CDP技术原理

CDP——Continuous Data Protection



■连续的工作（Continuous）

- 数据连续的写入主盘的同时写入CDP设备Host writes to primary data disk
- CDP设备的日志区记录所有数据变更

■CDP 日志

- 日志跟踪数据的变化
- 快照记录特定的时间点数据

■镜像

- 全部独立于生产数据
- 通过日志更新数据

■快照代理

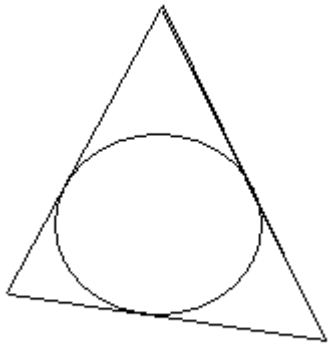
- 快照代理可以用来快速恢复数据库，邮件和文件系统到某一时间点
- 逻辑资源的数据一致性

■恢复（Recovery）

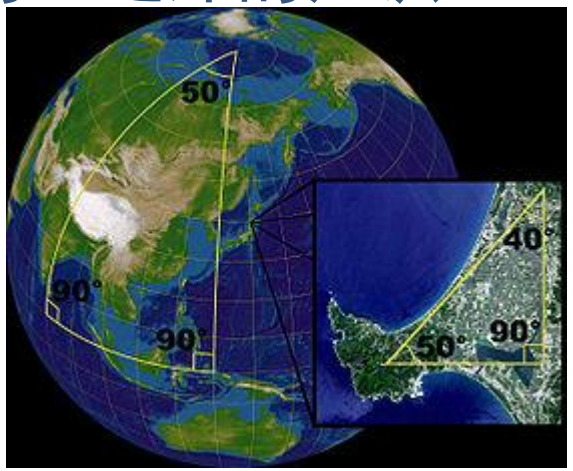
- 快照可以用来恢复到较长的某一时间点（小时，分钟）的数据
- CDP Journal 可以用来恢复到时间比较近的某一秒钟的数据

查找故障的根本原因

- 基础架构、网络、设备、开发、系统软件、运维同时查可以快速定位故障点，联合诊断有利于找出故障原因；
- 不放过任何的蛛丝马迹（以下为测试内容）
  - 三角形减去一个角至少还剩下几个角？
  - 是否存在“会的”和“不会的”之外的知识？
  - 三角形的内角和是多少？



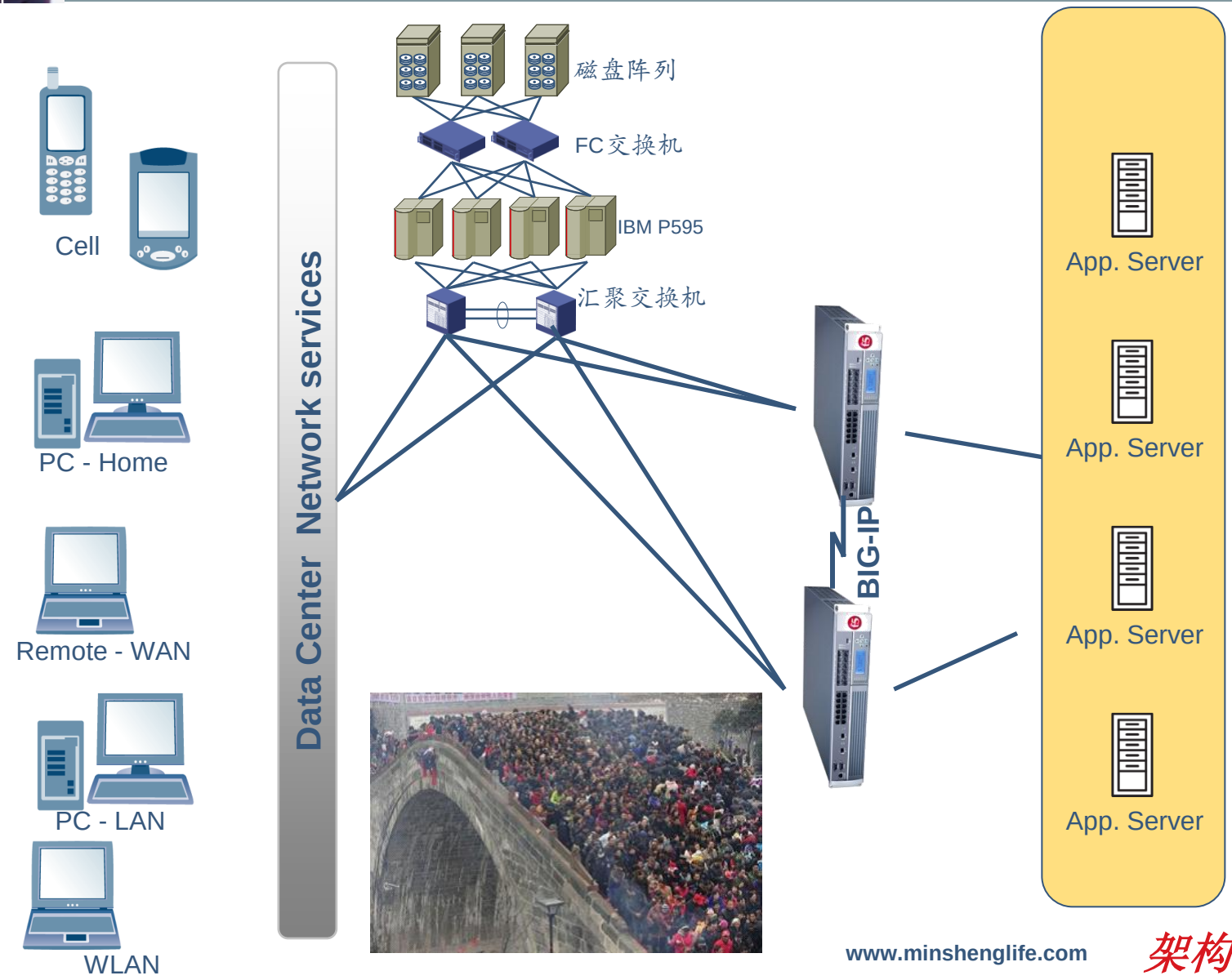
知识
- 未知
- 已知
  - 不会
  - 会的



故障定位——案例(存储、数据库)

- 换了更好的存储设备，数据库性能下降
  - 原因：新设备单盘容量增大（146→300）IOPS没变
- 数据库空间不够了，性能也差，新设备没到位
  - 原因：碎片严重，2011年7月，400GB→110GB

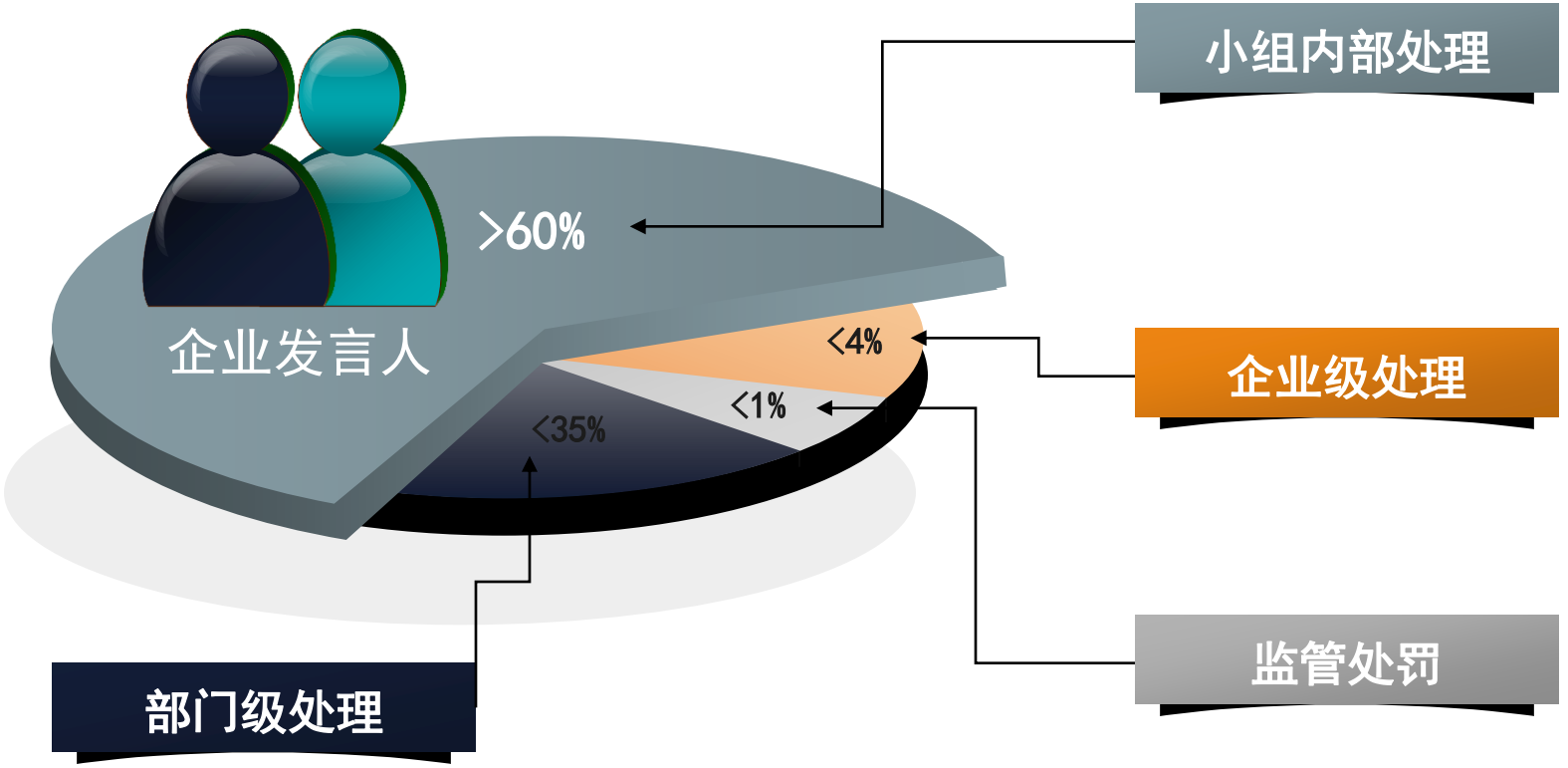
故障定位——案例（网络）


Cell
PC - Home
Remote - WAN
PC - LAN
WLAN
Data Center Network services
磁盘阵列
FC交换机
IBM P595
汇聚交换机
BIG-IP
App. Server
App. Server
App. Server
App. Server

故障的披露——话术技巧的应用

故障披露

是故障处理的关键环节之一，因披露的对象不同而方法各异。



利用发布的基础——共同知识

- 信息不对称
- 以共同知识为基础

知识{未知；已知{不会；会的}}

  - 共同知识是《博弈论》的基础，是数学的一个分支，在越是复杂的社会环境里面运用越广泛。
- 为正确的人办正确的事

  - 在不可靠通道下身份的确认
- 有时候故意卖破绽也是手段
  - 不便于披露而又想办法披露的手段

共同知识案例——QQ防盗术

妻子：我新买了号码，抽空给充50块，号码是13XXXXXXX。

丈夫：一会儿去。送给美姑娘的裙子买了吧？

妻子：我没空，还是你买吧！

结论：这个号被盗了！

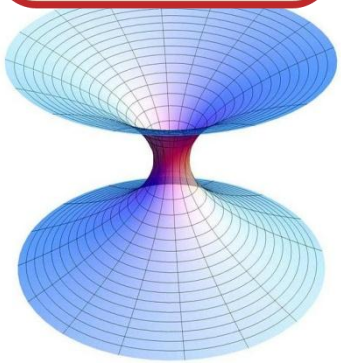
共同知识案例——实在不行也要留痕

XXX公司故障报告

201X年08月18日XX系统大面积故障原因查明：XX设备管理员证实，该故障为网线松动所引起，持续时间15分钟，重启设备后恢复。

XXXX公司信息中心

201X年05月21日



Thank You !

www.minshenglife.com