

深入浅出 复合事件处理

避免发生
资金损失



进行系统
动态校验



察觉威胁
消除隐患

正确预测
股票涨跌



发现老公
可能外遇



了解总督系统
独到之处



其实你每天都在做CEP

只是你不知道而已...

这就是人肉CEP



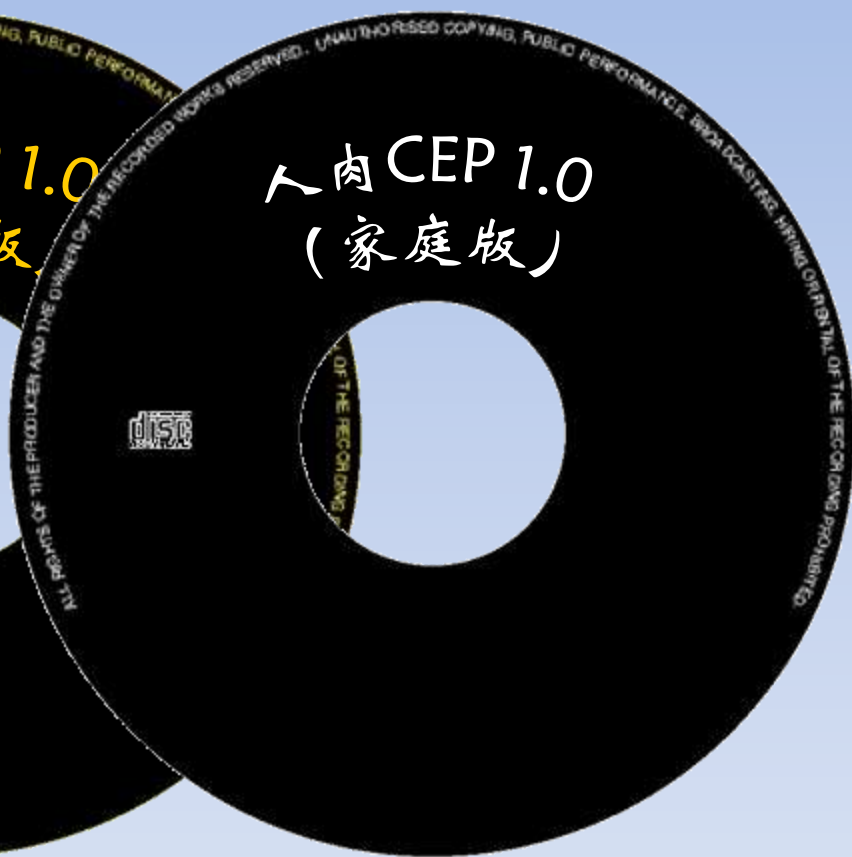
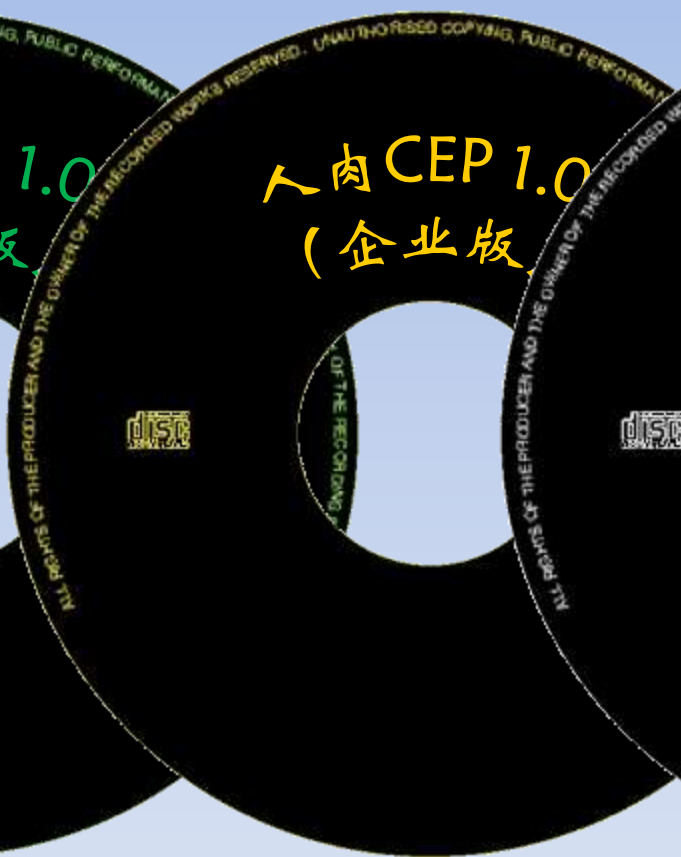
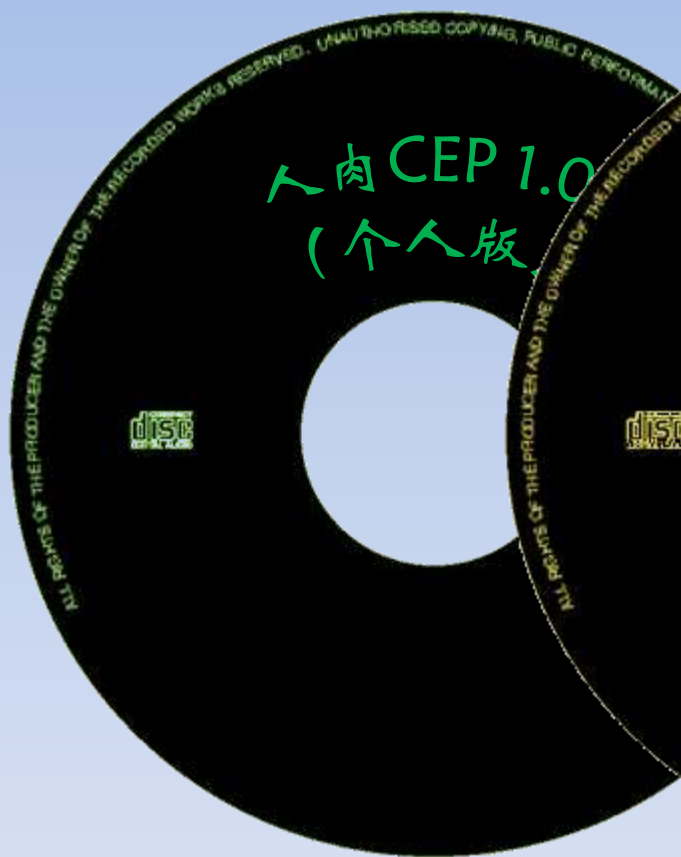
感知

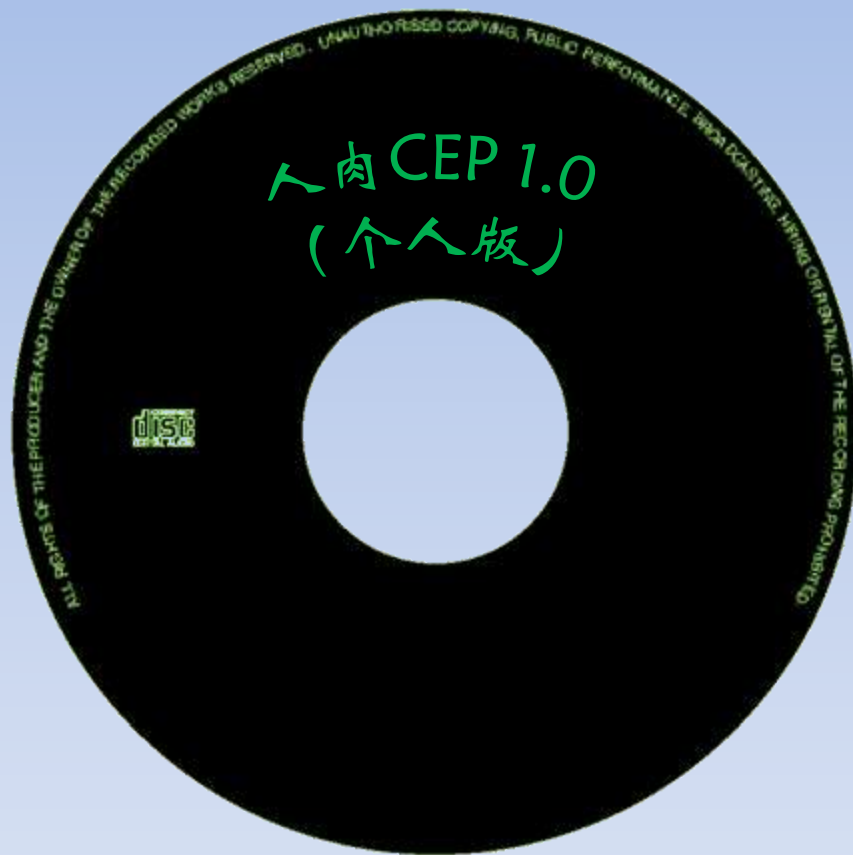


判断



行动





人肉 CEP 1.0
(个人版)

disc

基础事件1：皮肤感觉温度下降

基础事件2：鼻子感觉湿气很重



基础事件3：耳朵听到远方雷声

基础事件4：眼睛看到乌云、闪电



The background of the slide is a dense field of blue water droplets of various sizes, creating a textured, bubbly appearance. A dark grey horizontal bar is positioned across the upper portion of the image, containing the text.

复合事件：即将下雨

因应之道：出门要带伞





人肉CEP 1.0
(企业版)

disc

ALL RIGHTS RESERVED. UNAUTHORIZED COPYING, PUBLIC PERFORMANCE, REPRODUCTION, RENTAL OR LENDING OF THE RECORDING PROHIBITED.

基础事件1：看到员工经常有一堆事没做完



基础事件2：看到员工经常上班时偷菜



复合事件：该员工不胜任

因应之道：FIRE他



人肉CEP 1.0
(家庭版)

disc

ALL RIGHTS OF THE PRODUCER AND THE OWNER OF THE RECORDING WORKS RESERVED. UNAUTHORIZED COPYING, PUBLIC PERFORMANCE, BROADCASTING, RENTAL OR LENDING OF THE RECORDING PROGRAM PROHIBITED.



基础事件：老公老说要加班

哪有公司这么常加班的？

基础事件：我感觉他在外面洗过澡

还说没有，明明就有肥皂味！



基础事件：衣服上沾粘长头发

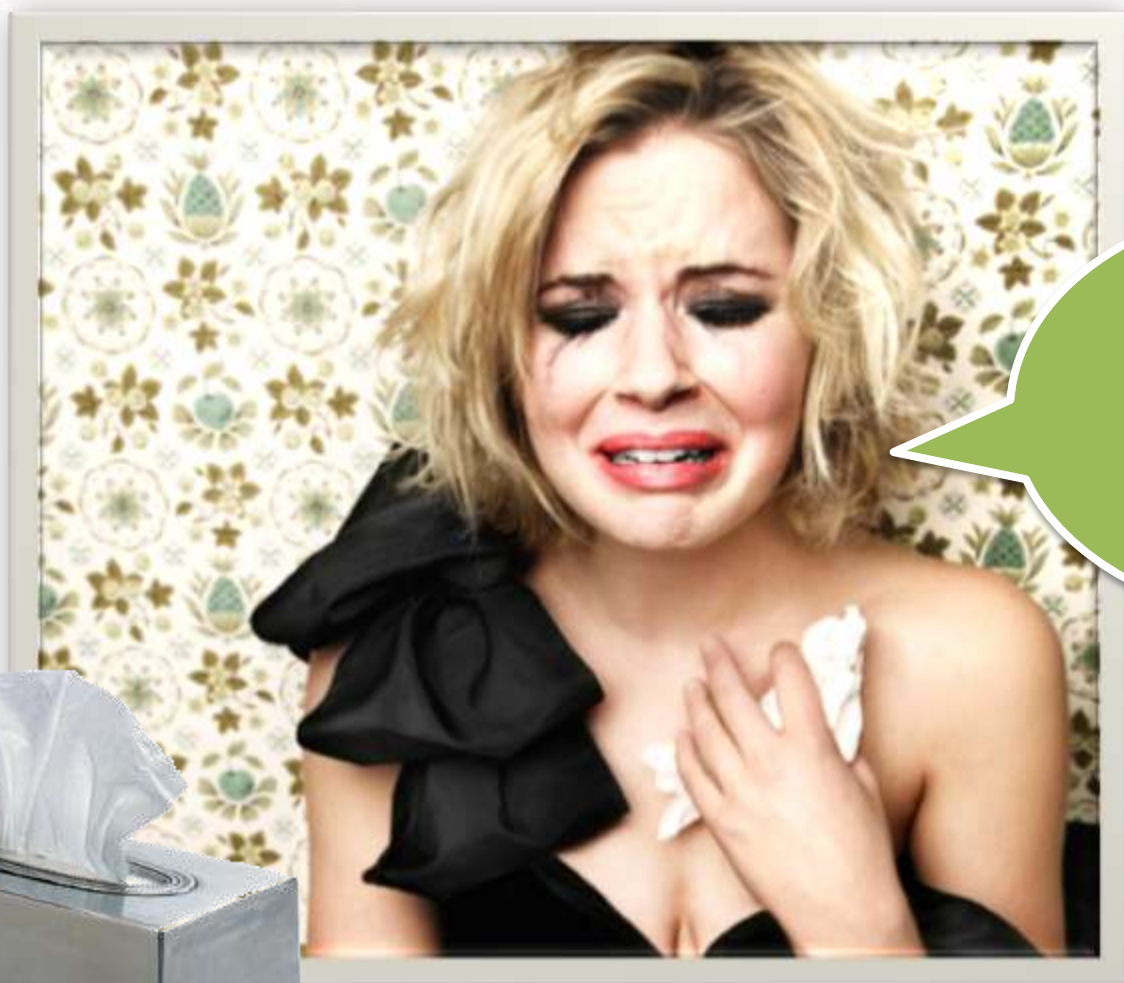
我的头发可没这么长！

基础事件：对我性趣缺缺

我都打扮成兽兽了耶！



复合事件：老公有外遇



他包二奶
了啦!



提醒：别急著下毒手，误报警率可能很高



冤枉呀！

因应之道：雇用「捉猴」侦探跟踪他



看了这么多比喻
应该能体会CEP了吧！

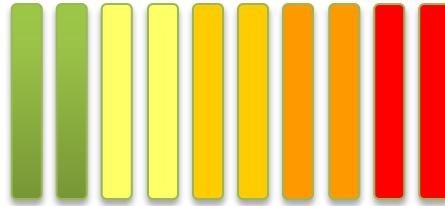


事件捕获

困难度 

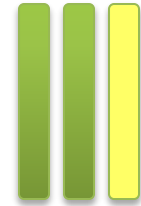


事件分析

困难度 



事件因应

困难度 

IT

其实你每天都**能**做CEP

只是你不知道而已...

这是一个IT事件爆发的时代



ERP

Oracle

SCM

RFID

每个系统都会产生大量的事件

CRM

Cloud
Computing

IBM

E-Mail

PeopleSoft

IM

B2B

Microsoft

Web

BAM

B2C

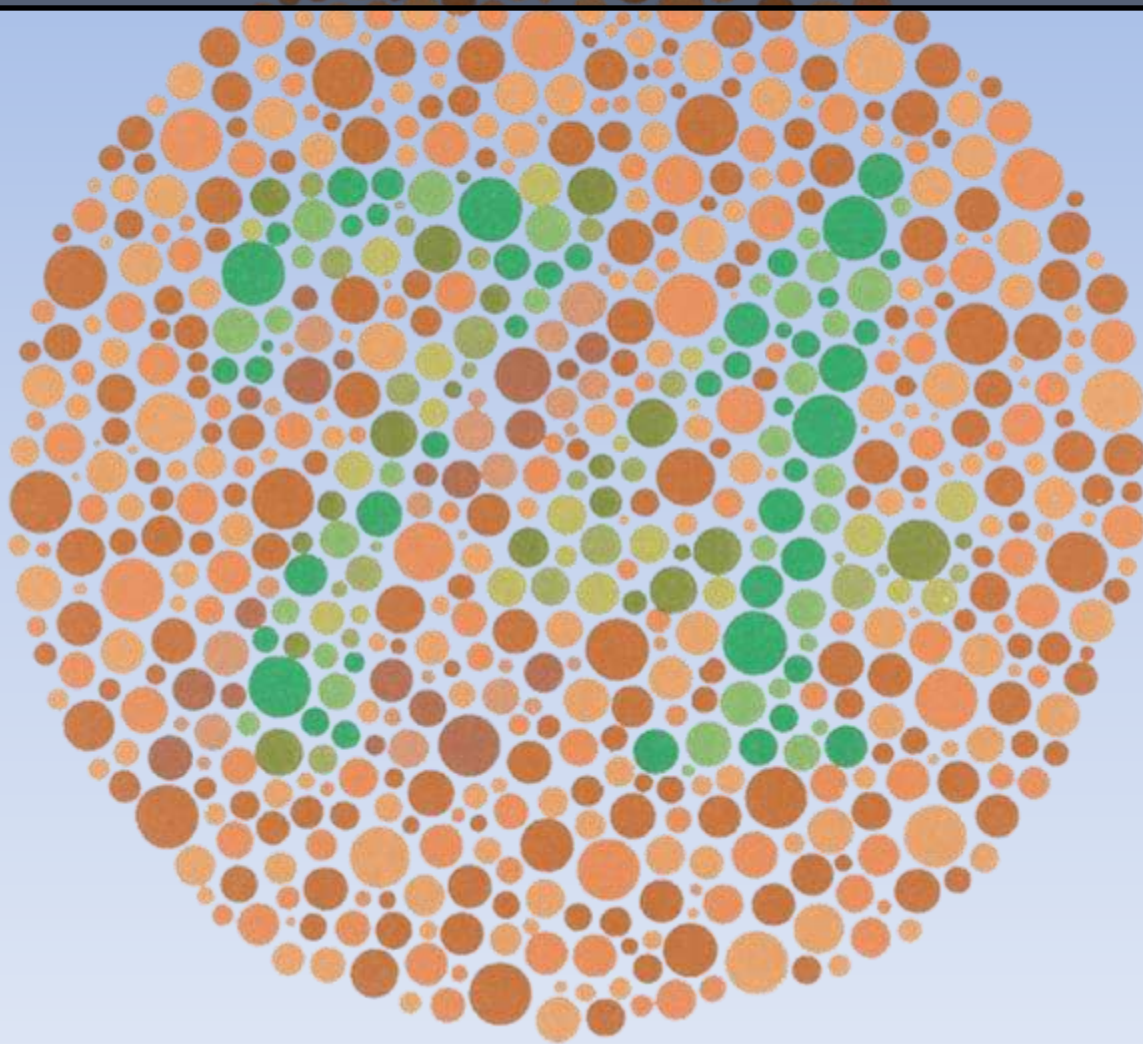
SAP

但我们一股脑儿把事件全扔了！



IT
事件垃圾桶


事件盲 (Event-Blind) : 对事件视而不见



承认吧！ 现况就是如此！

我们



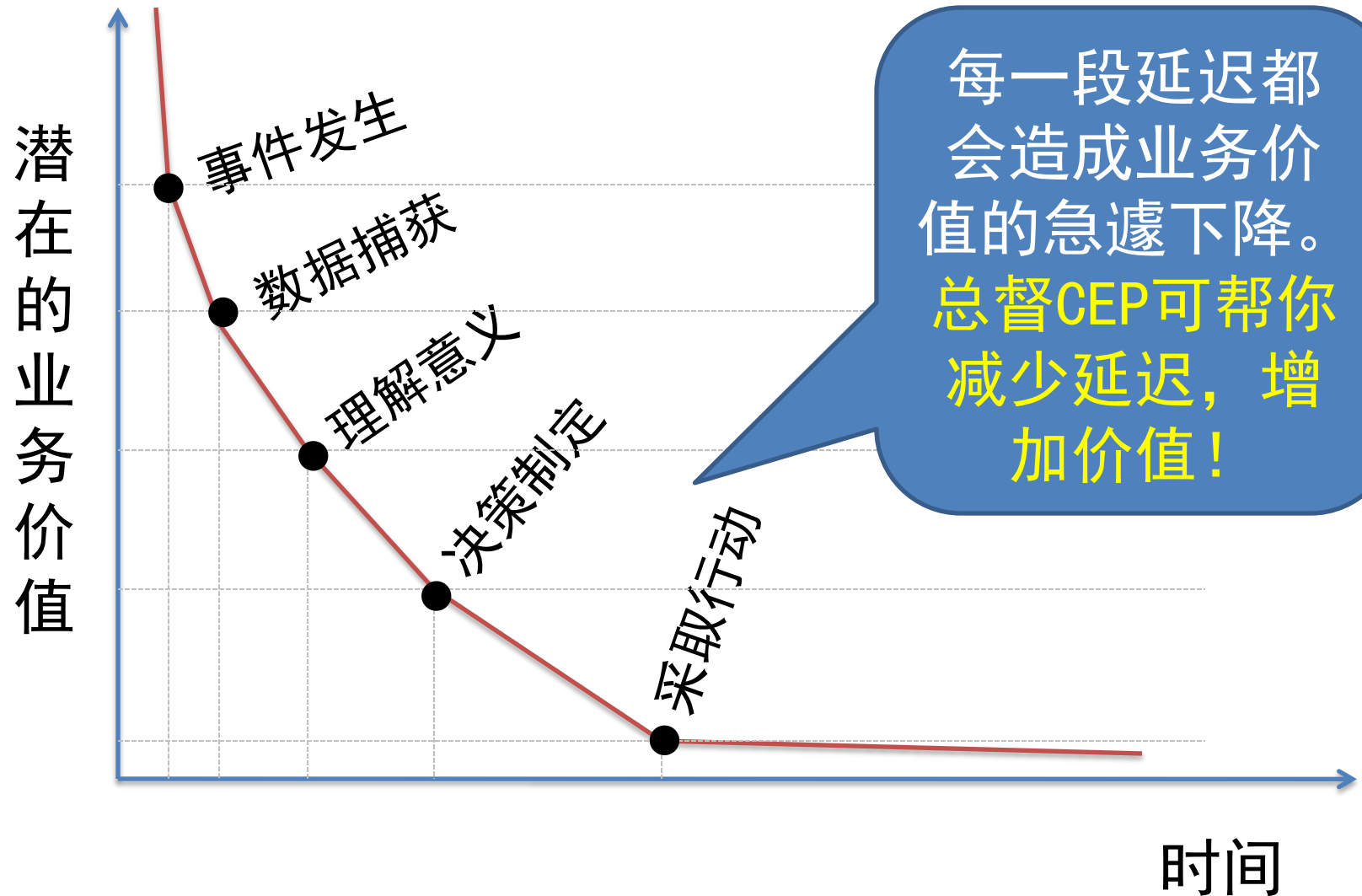
A photograph of two men in suits at a formal event. The man on the left, with dark hair, is saluting the man on the right, who has grey hair. They are surrounded by other people in uniform and flags.

我发誓要改变现状，开始重视复合事件。

简单！参加
总督CEP系统
的监控就行了！

广告时间

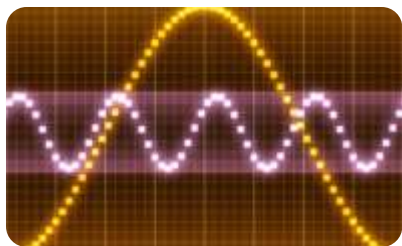
总督CEP：减少延迟，增加价值



CEP应用领域



商业活动监控



群众智能



业界应用



网络攻击



犯罪预防



系统动态校验

支付宝使用CEP



对外，防止犯罪

网络诈欺、网络攻击、洗钱防治



对内外：防止资损

银行、商户、用户错帐；内部错帐



对内：业务状况监控

趋势因应、营销决策、风险规避



商业CEP产品



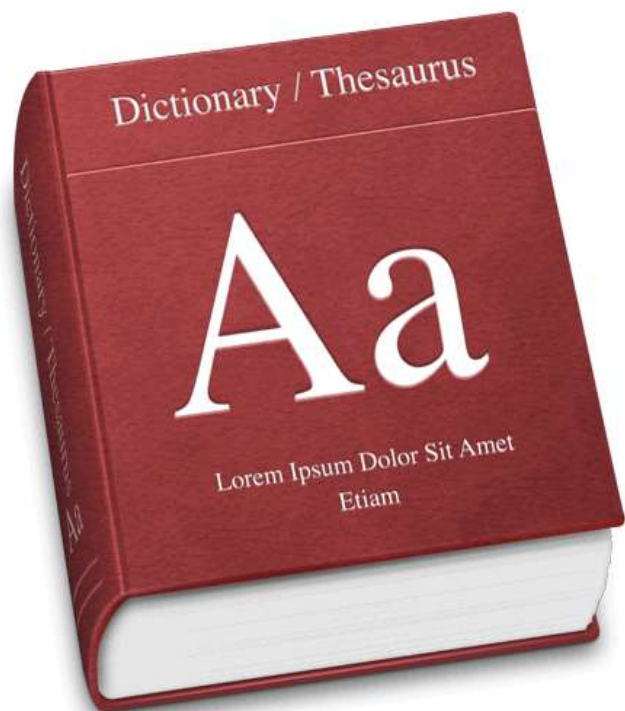


难得有微软没做的领域？

微软即将推出StreamInsight

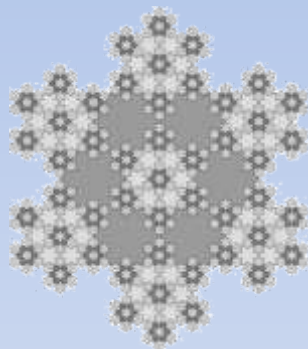
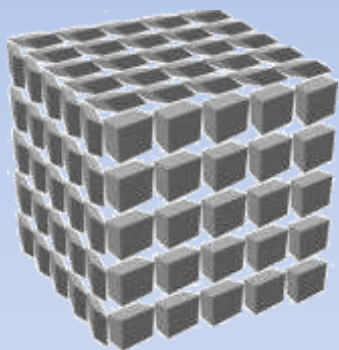
CEP关键技术

CEP 关键字



- Streaming
 - 连续不间断
 - 实时处理
- Base
 - 资料量大
 - 数据库
- Insight
 - 有用的信息
 - 智能

CEP关键过程



格式化

预处理

模式侦测

事件发派

报警

CEP关键模块



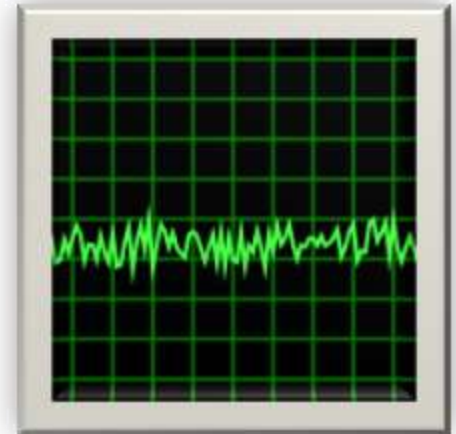
CEP辅助工具



规则制作工具

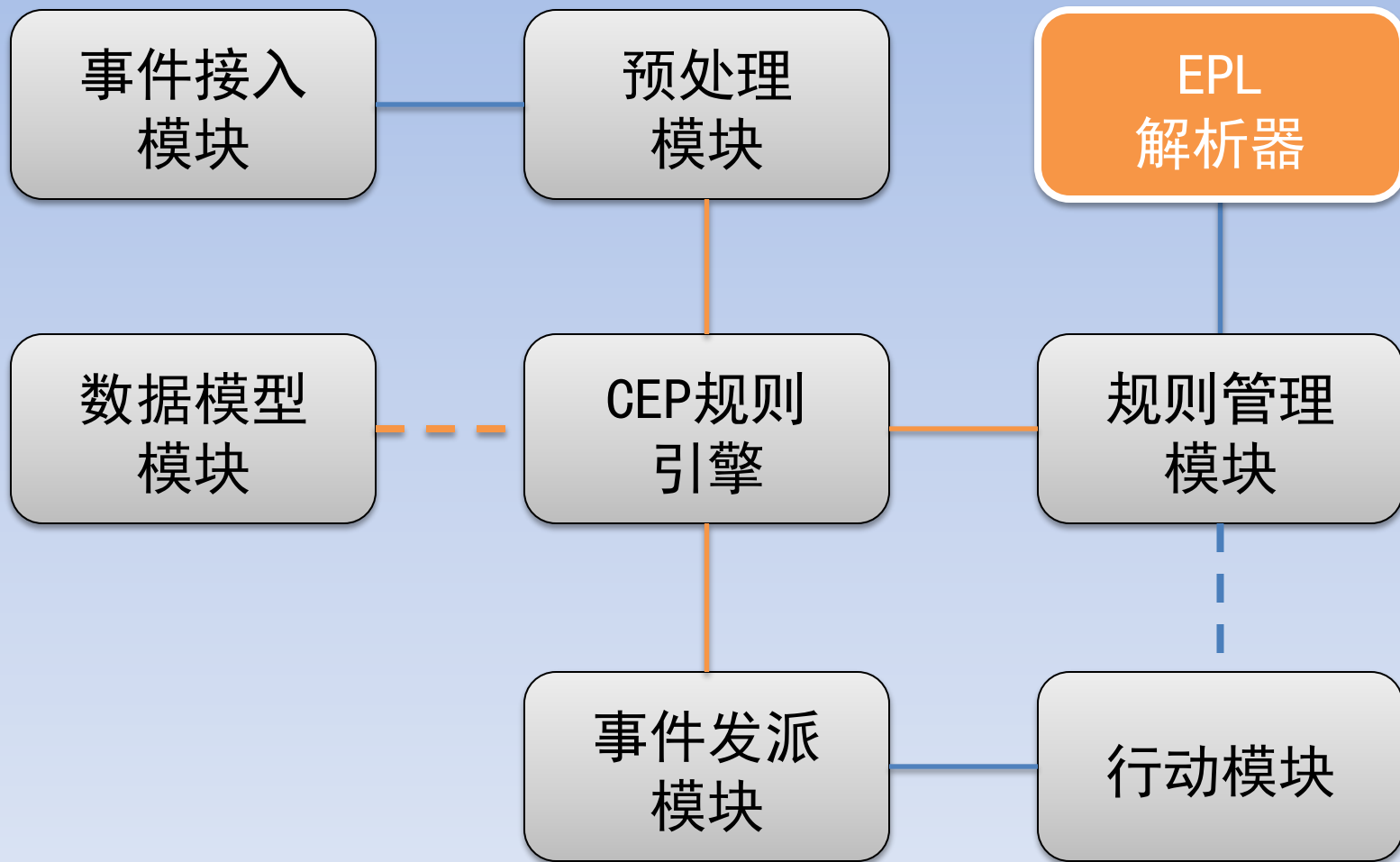


报表输出工具



实时仪表板

EPL解析器



EPL（事件处理语言）



理論上：

EPL
规则



EPL
解析器



内部
规则



实际上：

CEP-EPL

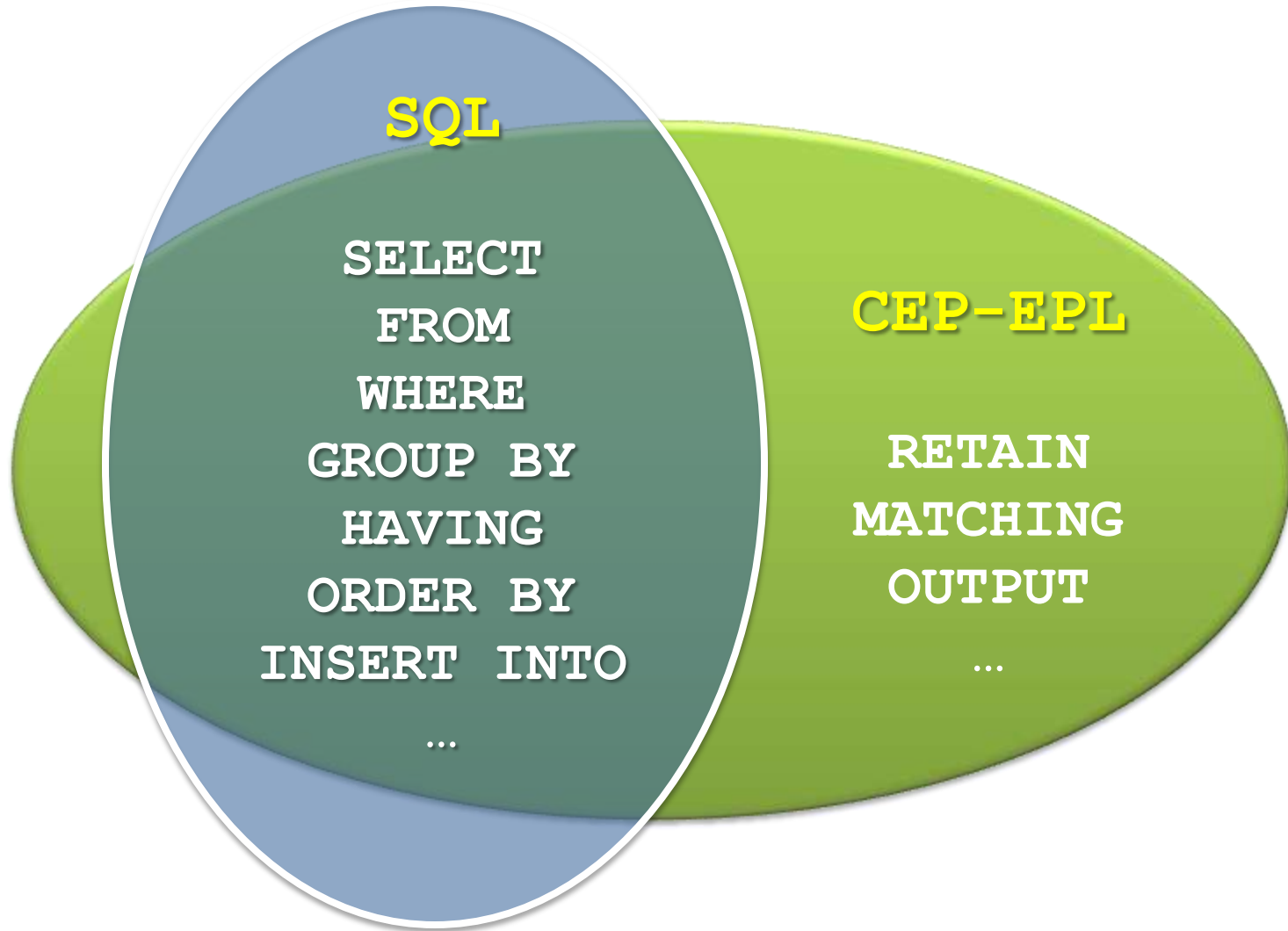


EPL
解析器

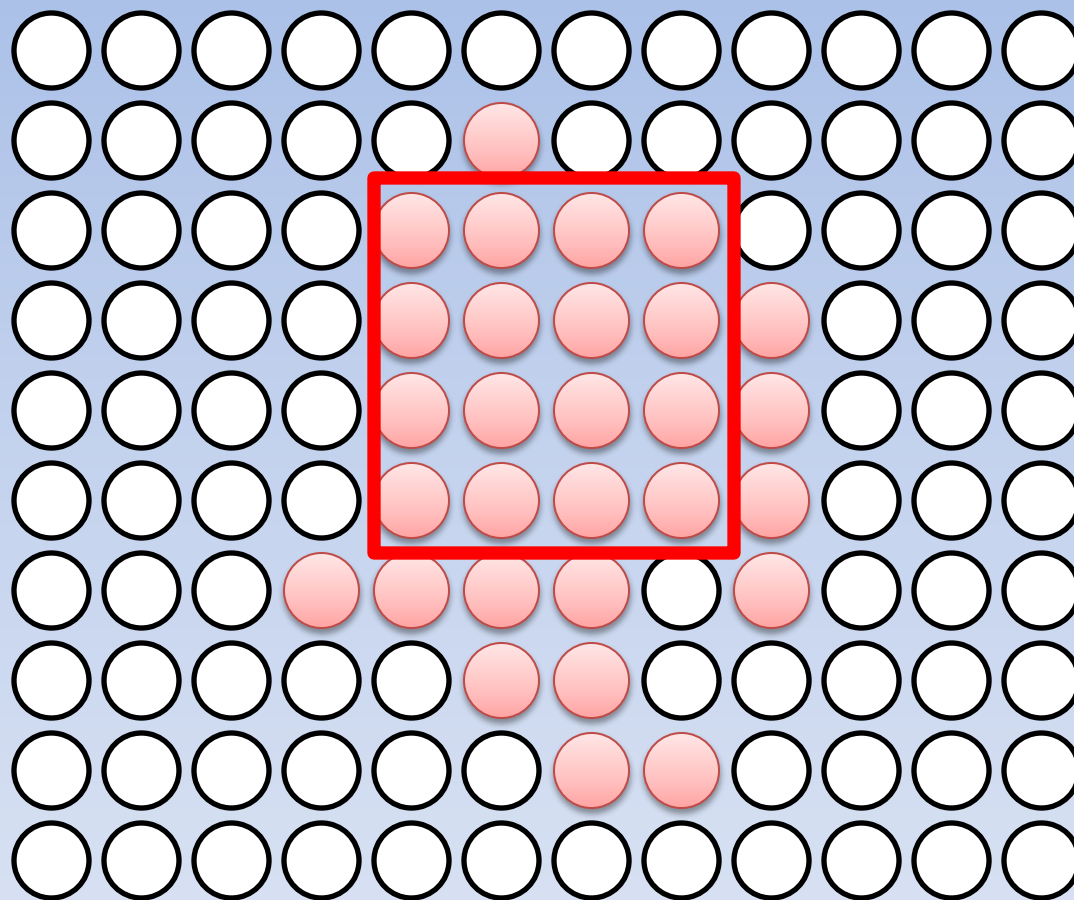


SQL/LINQ
命令、函数、
Trigger

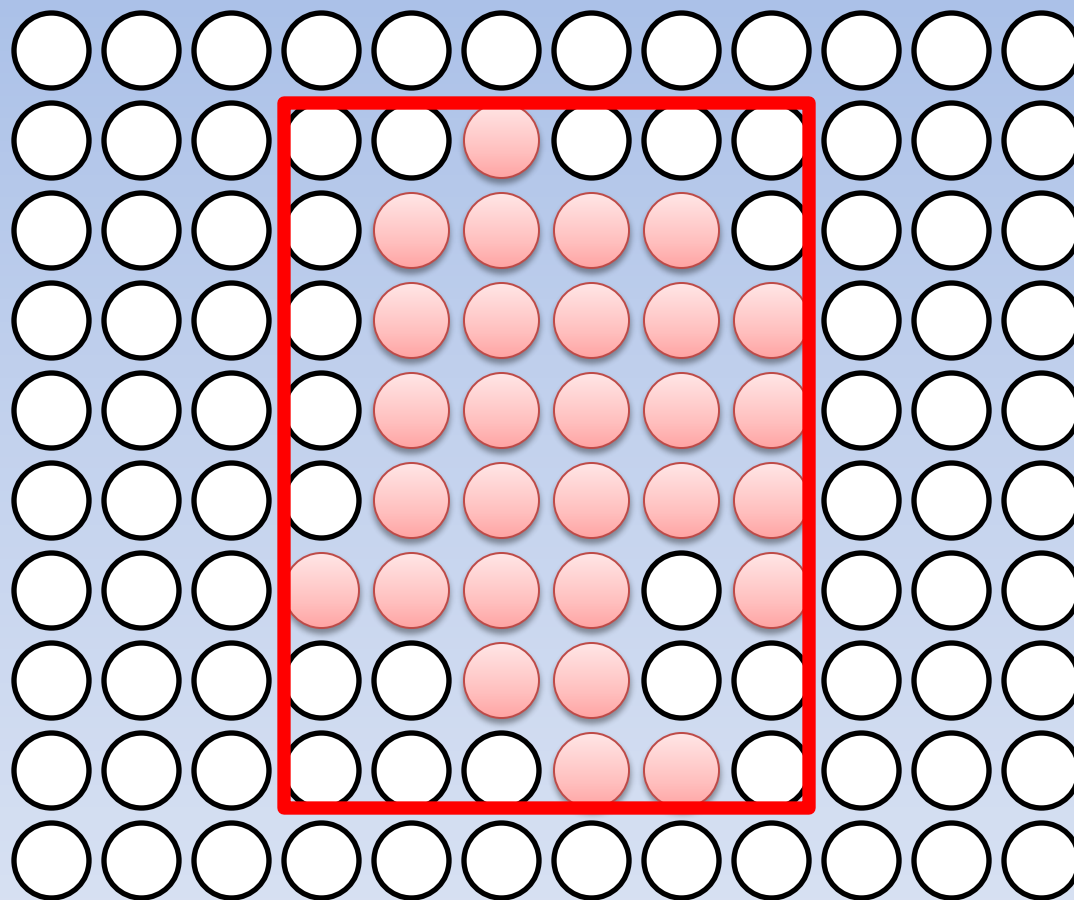
市面上CEP-EPL都是扩展自SQL



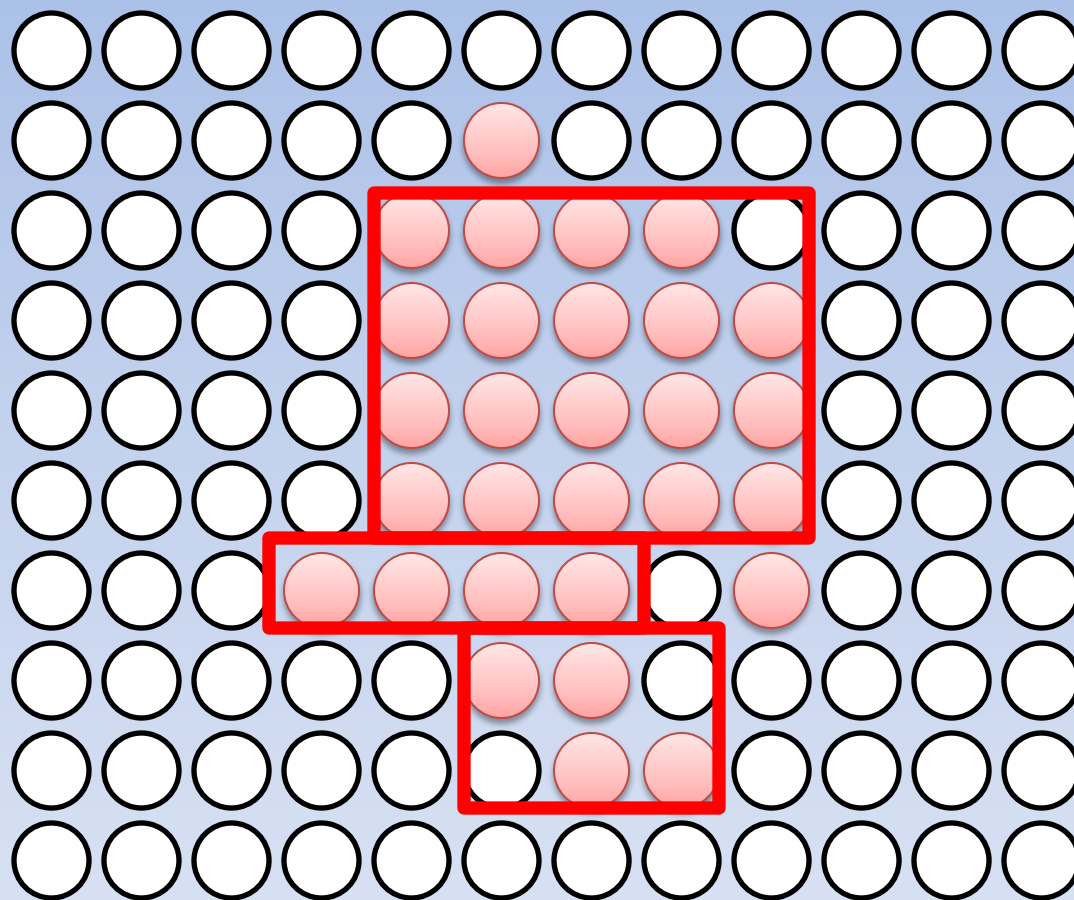
无误报警，但漏网之鱼很多...



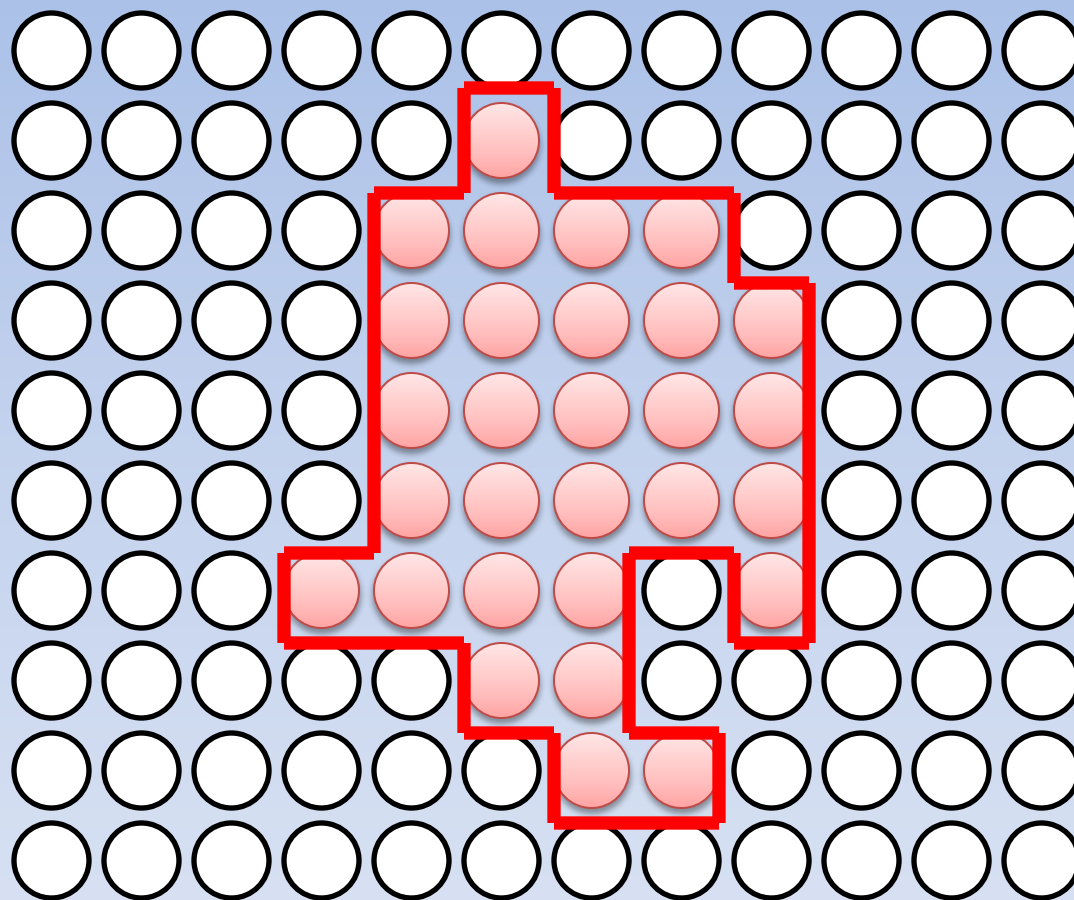
有误报警， 但无漏网之鱼



有误报警，漏网之鱼很少



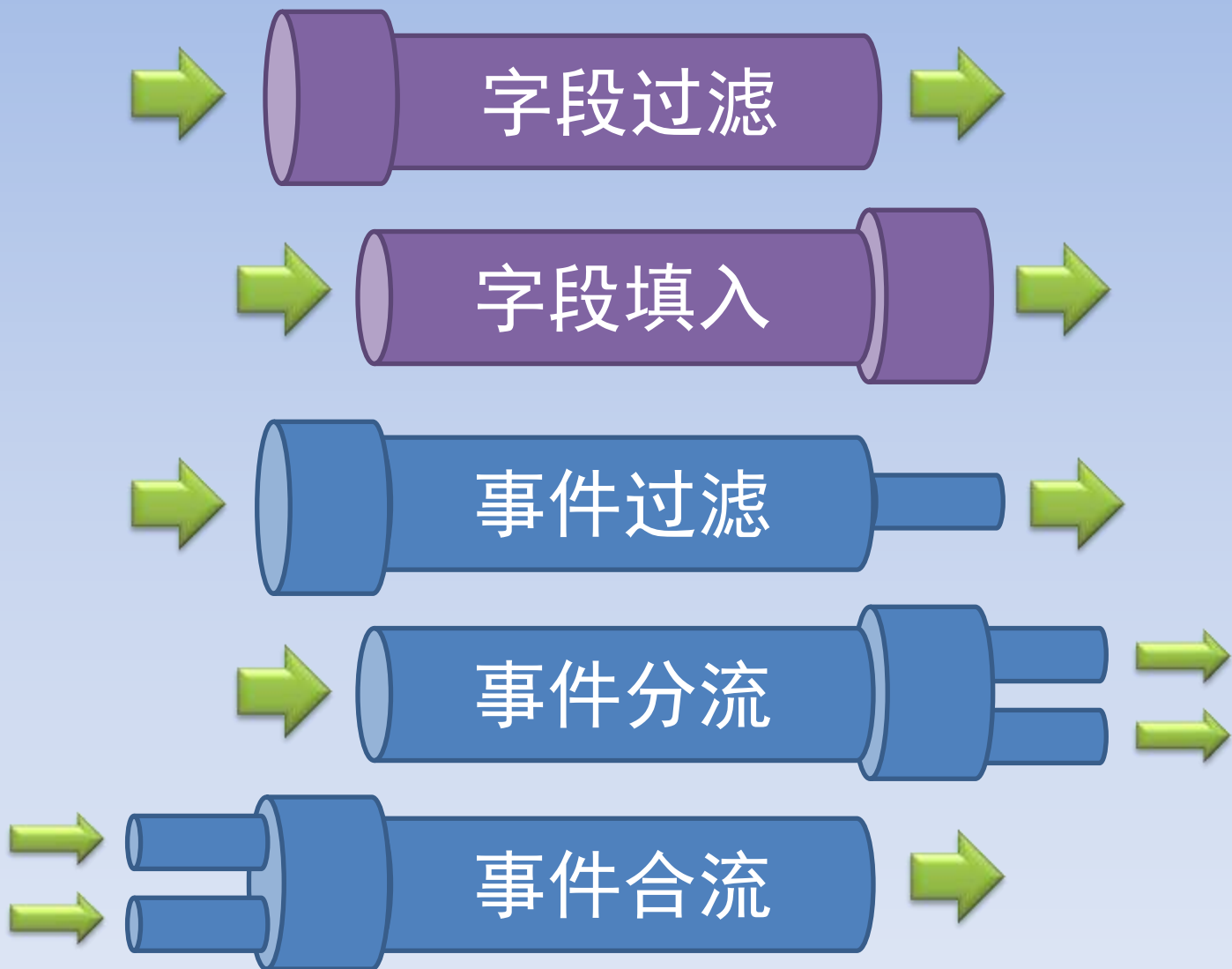
无误报警，无漏网之鱼… YA!



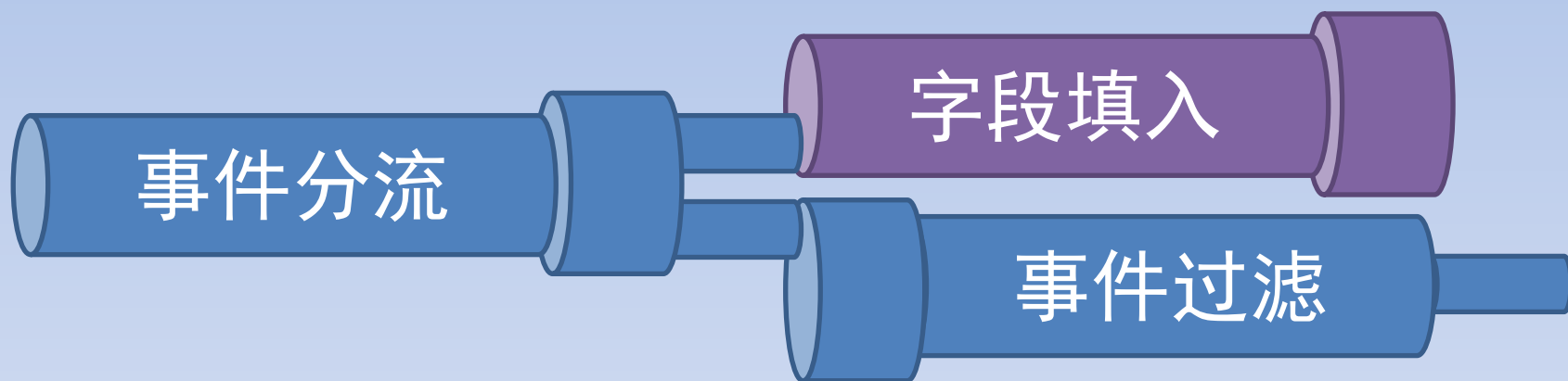
预处理模块



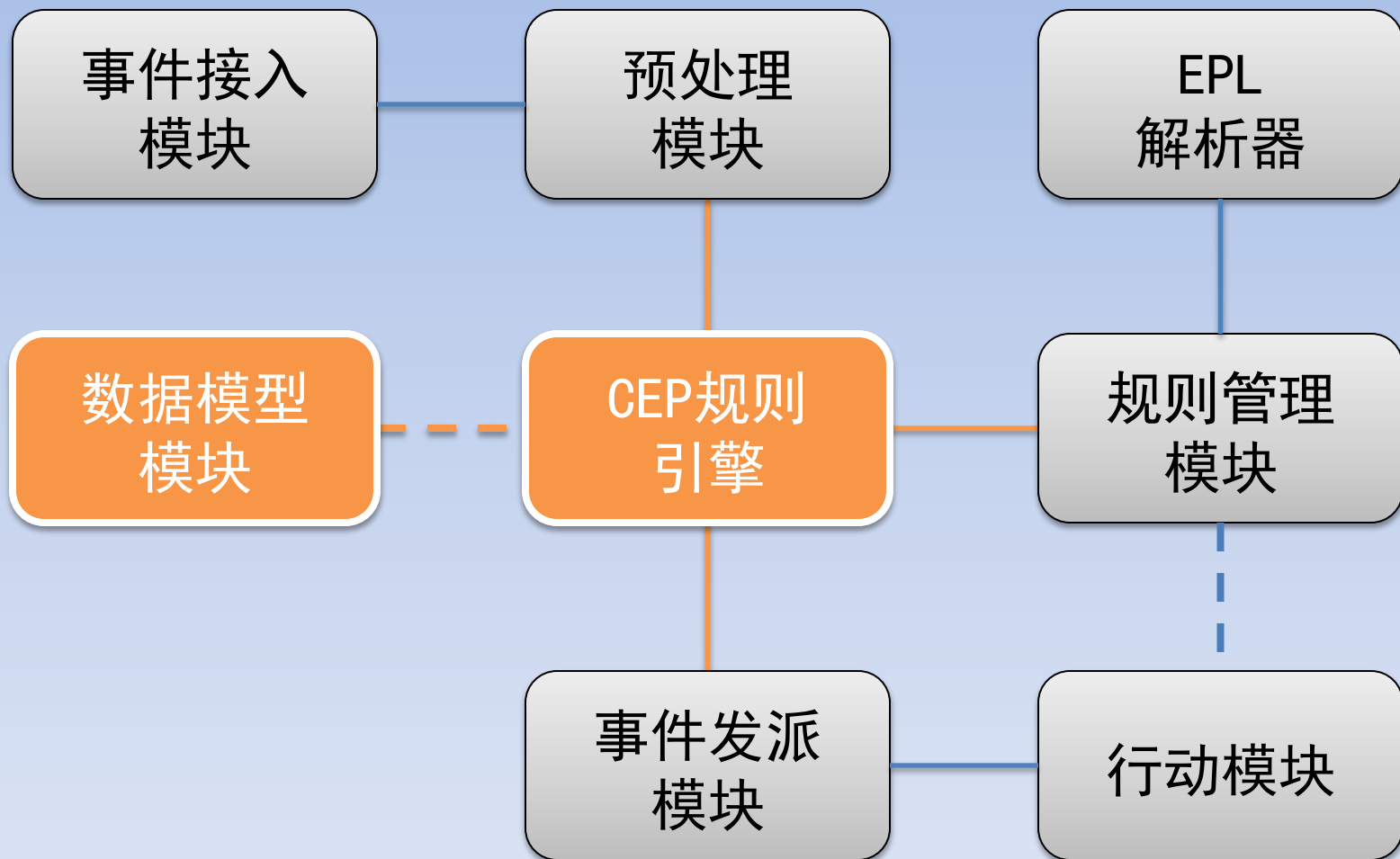
预处理模块采管线架构设计



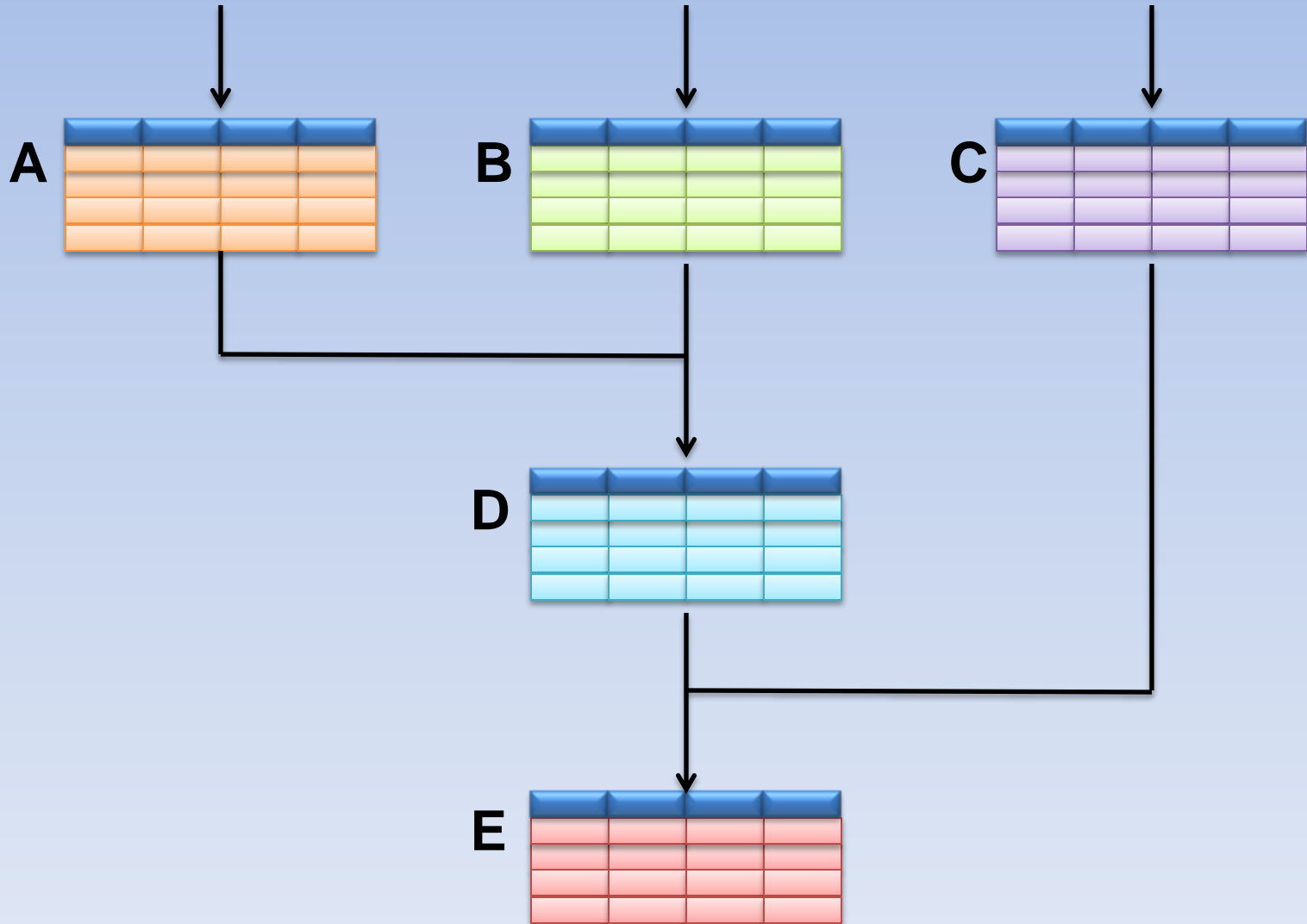
好处是…前后随你接



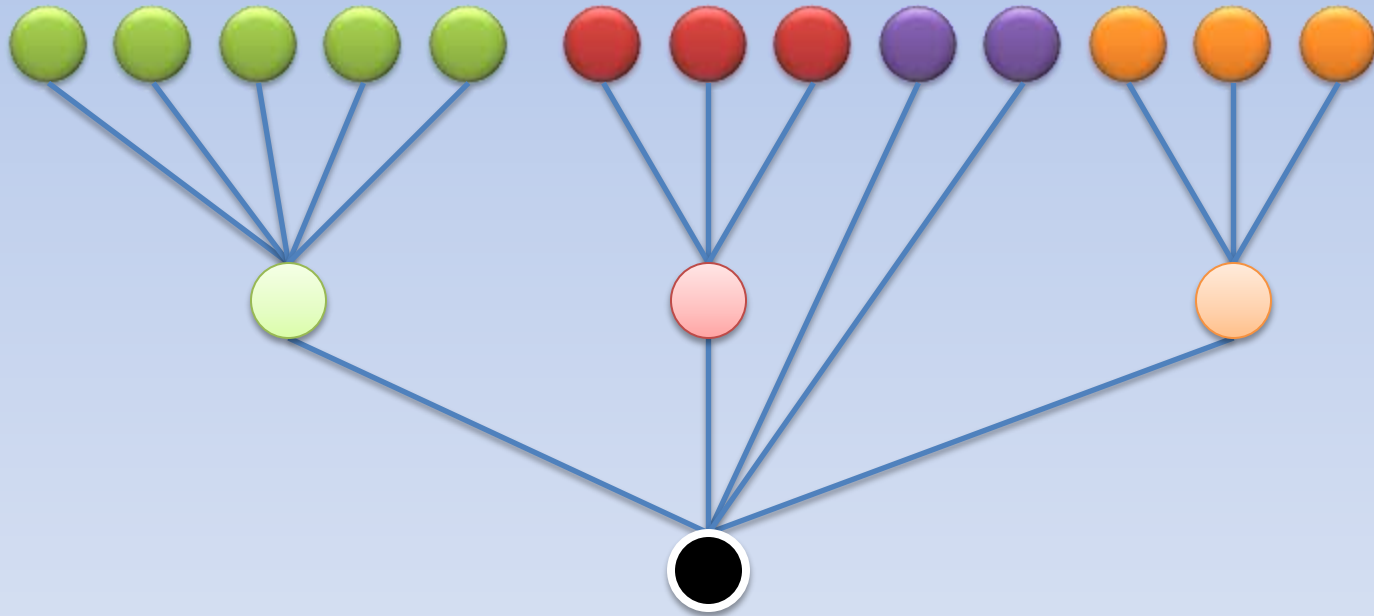
引擎与数据模型



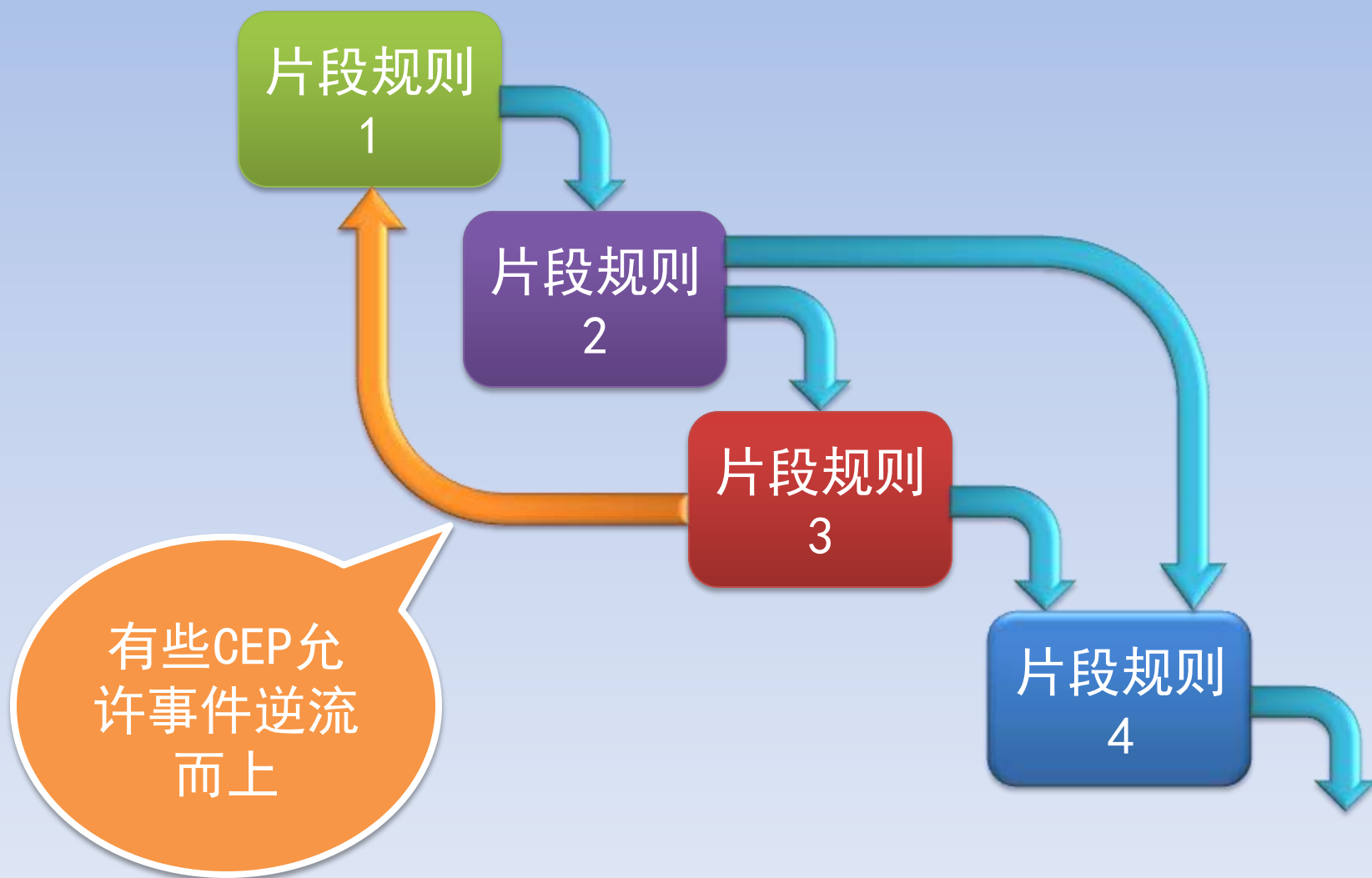
也可以多个表输入，一个表输出



复合事件的阶级

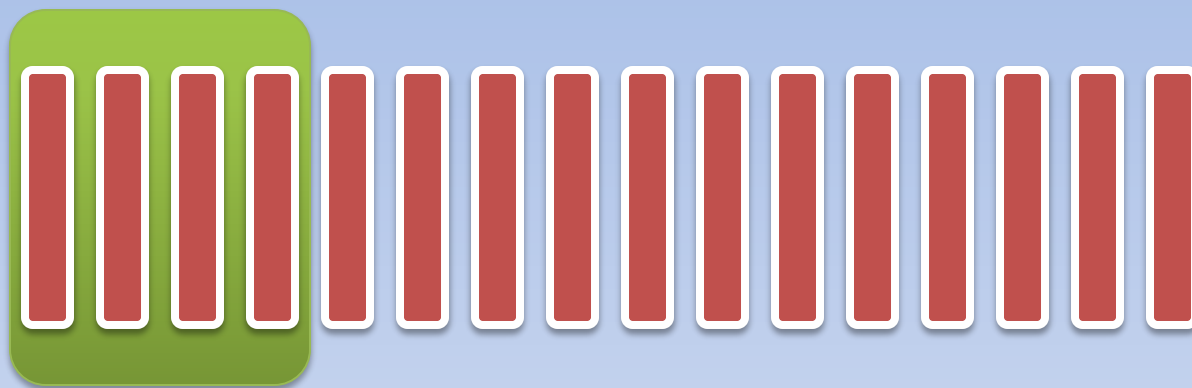


规则分解成上下游许多片段规则

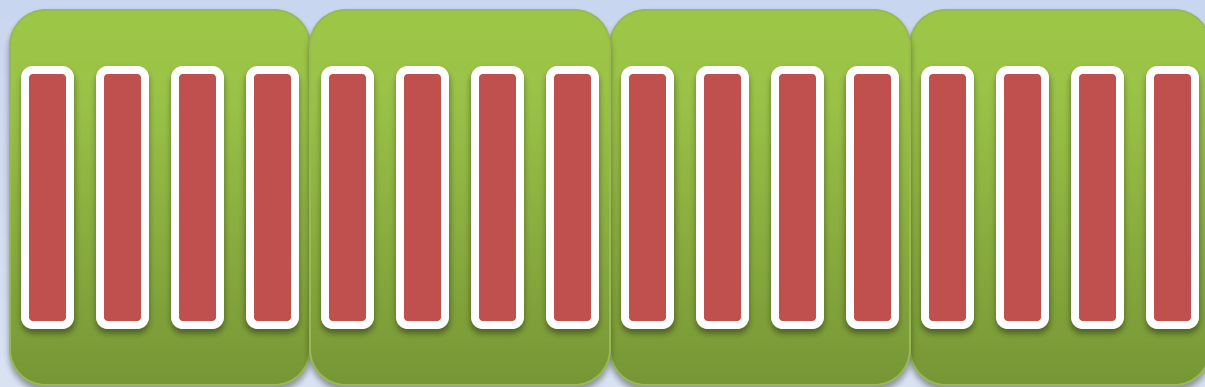


扫描方式：滑动与跳跃

滑动式
扫描

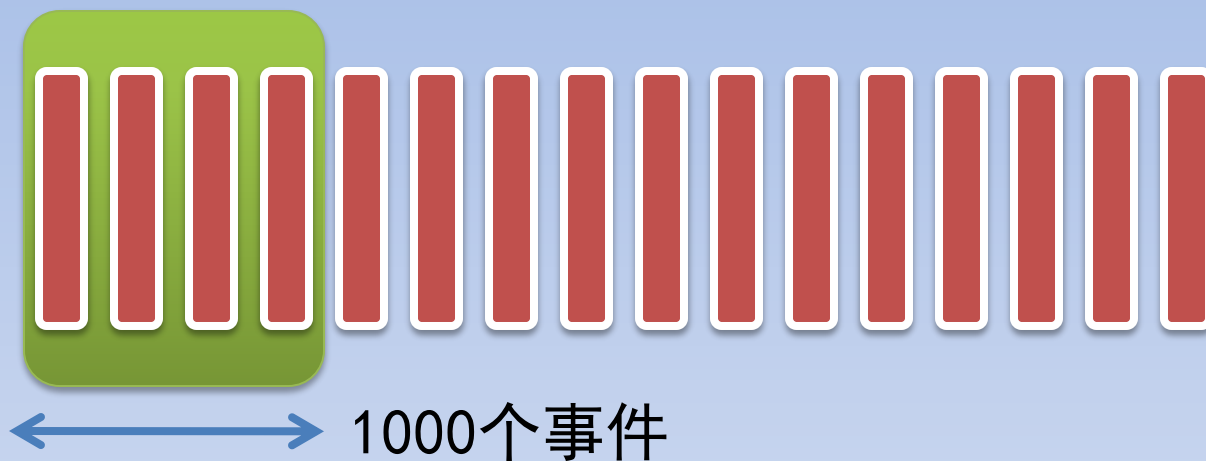


跳跃式
扫描

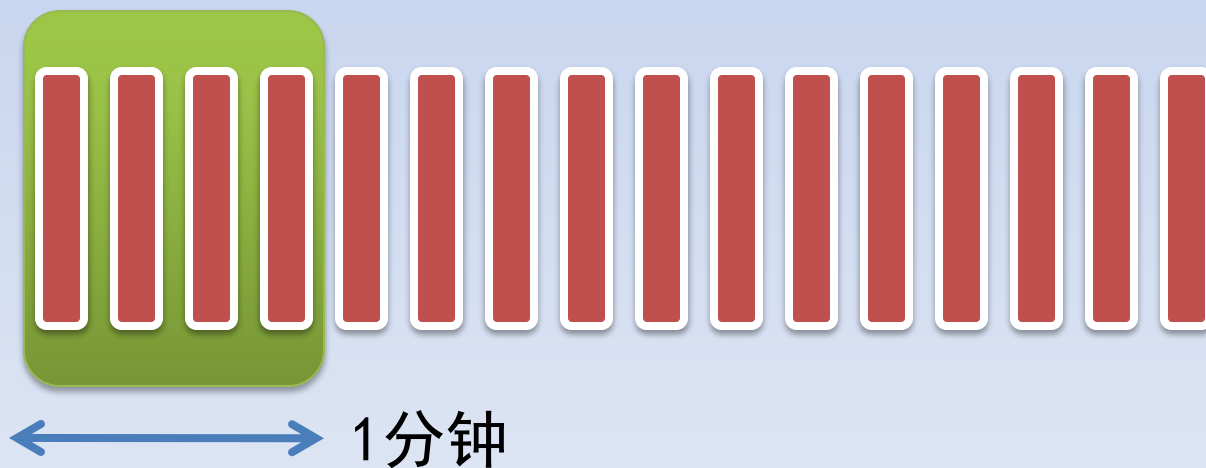


扫描区间：定量与定时

定量区间



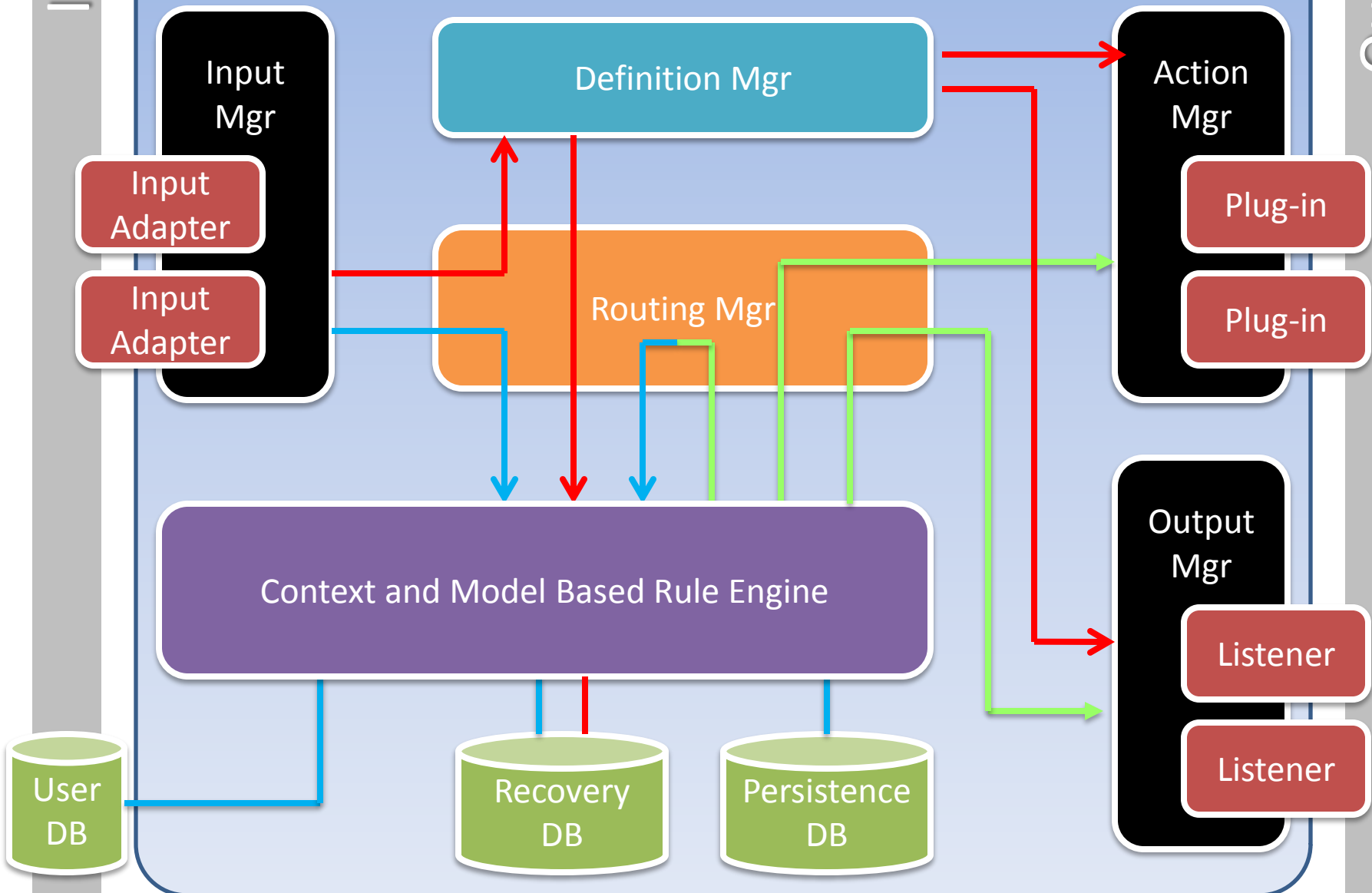
定时区间



Input

IBM Amit CEP Architecture

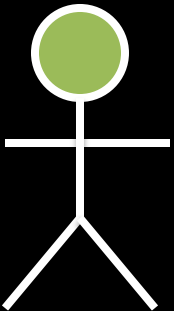
Output



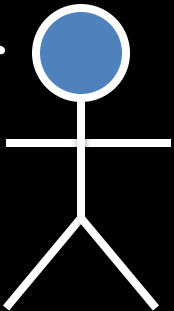
孔宣大人



【小品】
哥做的不是后督
是总督



我是
正牌总督



我是孔宣
(软件工程师)

升堂

威武 . . .

传犯人孔宣

本府为朝廷任命之正牌总督，但最近本府听说你自封为总督，你可知罪？

冤枉呀！总督大人。小的是负责软件开发的，原本要开发一套**后督系统**，以进行资损的监控，但因为此系统功能相当弹性而强大，可以督的事情不只资金的部份，所以小的随口将「后督」改名为「总督」罢了

哦！是这样嘛？那这套总督系统可以做那些事呢？

基本上，**BI（商业智能）、BAM（商业活动监控）、系统监控、网络攻击侦测、洗钱预防** … 等任务，大部分「总督系统」都能做到！

这么强大？不会只是
宣传噱头吧？

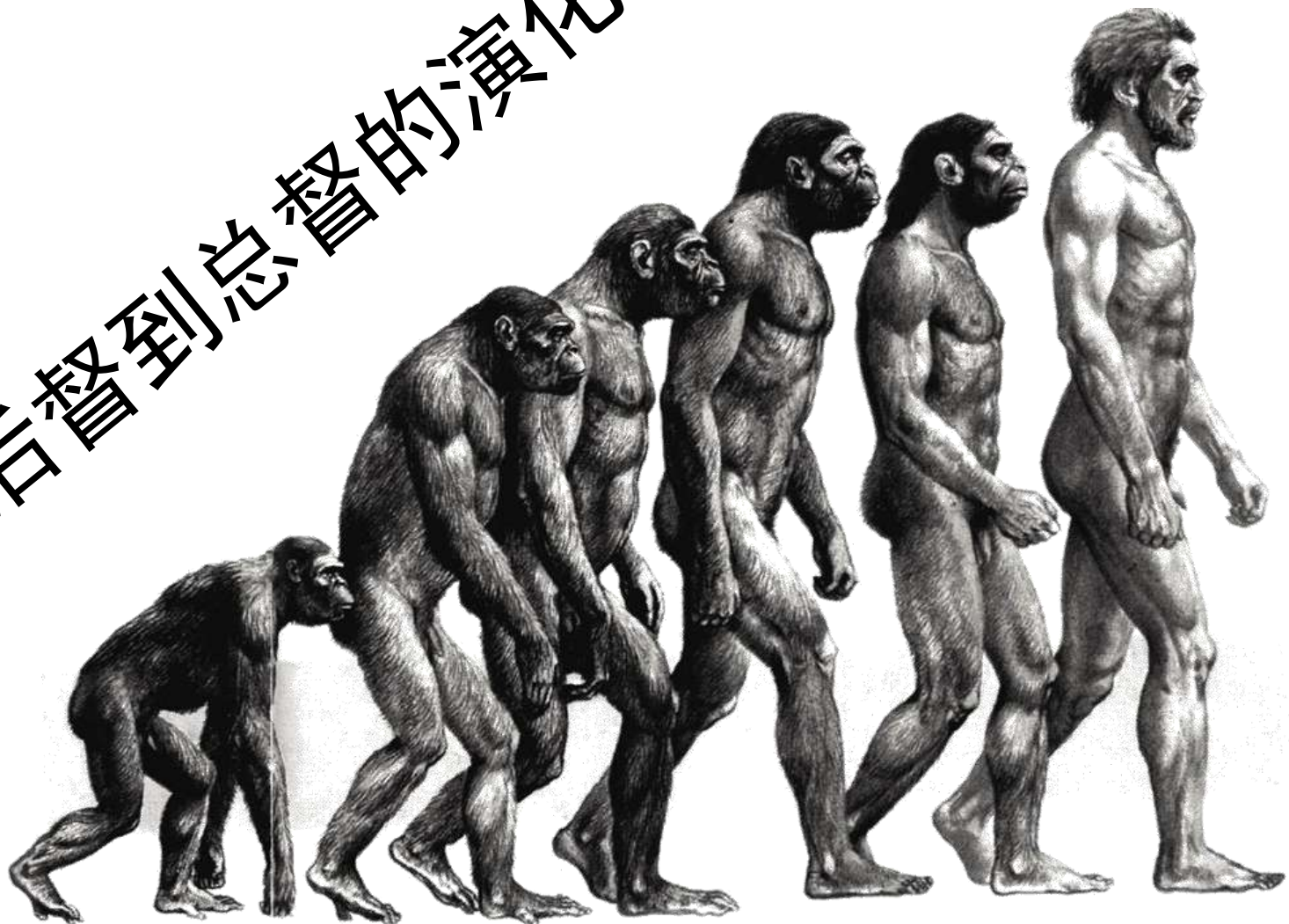
冤枉呀！大人。
总督系统通过**状态机引擎**运行监控规则，只要编写各式各样的总督规则，就可做各种不同的监控。而这总督规则就是程序，可以做任何的事，任何数学计算与逻辑运算都难不倒它。

这么强大，给本府一套玩玩。

大人你有所不知，因为小的编程能力有限，所以系统现在还有很多BUG，不太稳定。加上人力短缺，开发进度一直快不起来，估计最快还要两三季才能完善整个系统。

大胆刁民，藉口这么多，来人呀！拖出去斩了！

从后督到总督的演化



后督



EDA



数据库CEP



状态机CEP



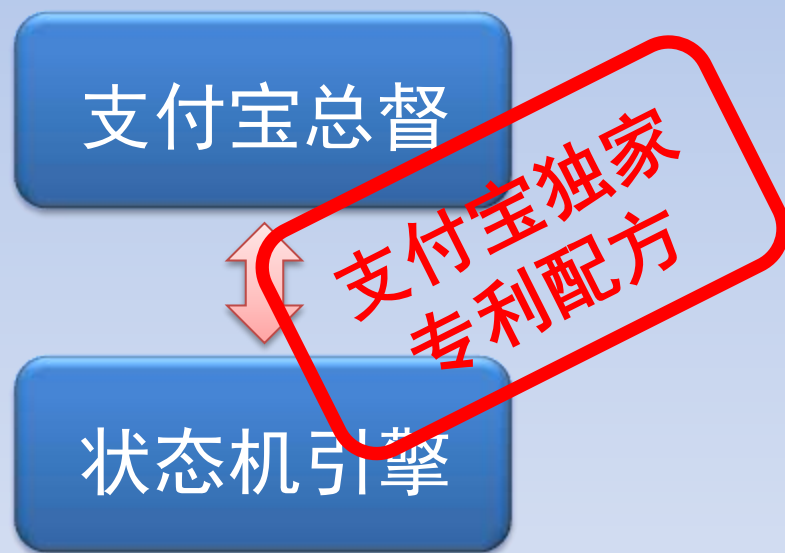
总督



Viceroy

支付宝 总督系统

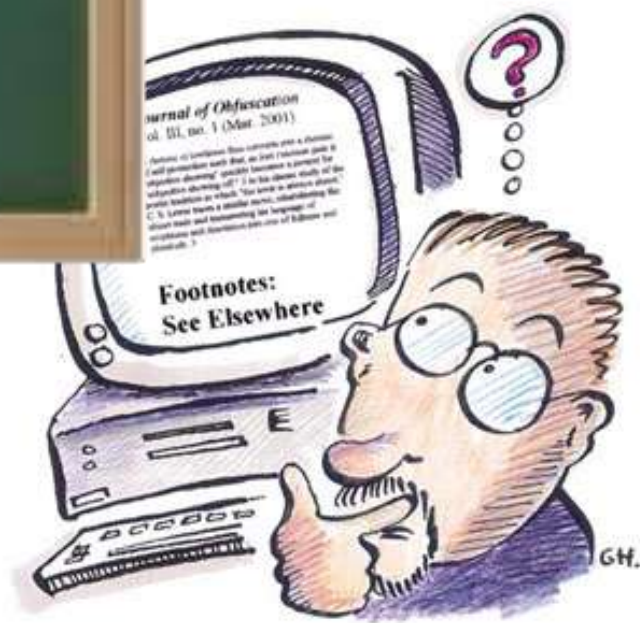
总督采用不同于其他CEP系统的设计



他牌CEP：笨重、庞大、僵化



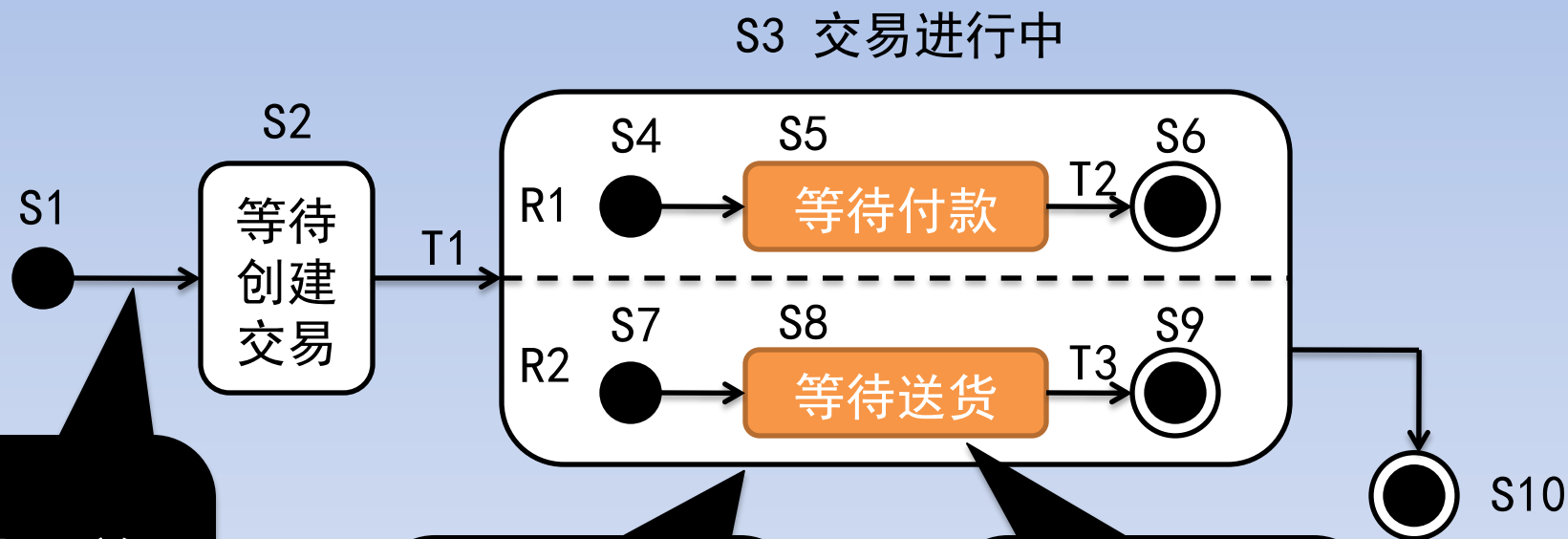
1. 他牌CEP无法（或难以）描述相当复杂的复合事件。
2. 他牌CEP事件格式受到数据库表schema的限制，无法自由扩展。
3. 他牌CEP需要大量的存储。



总督CEP：轻巧、敏捷、灵活



总督CEP状态机的好处



事件不放数据库，所以格式不受限制。

状态机相当灵活，描述能力很强。

只需记录当前状态，相当节省存储。

总督支持两种模式

模式



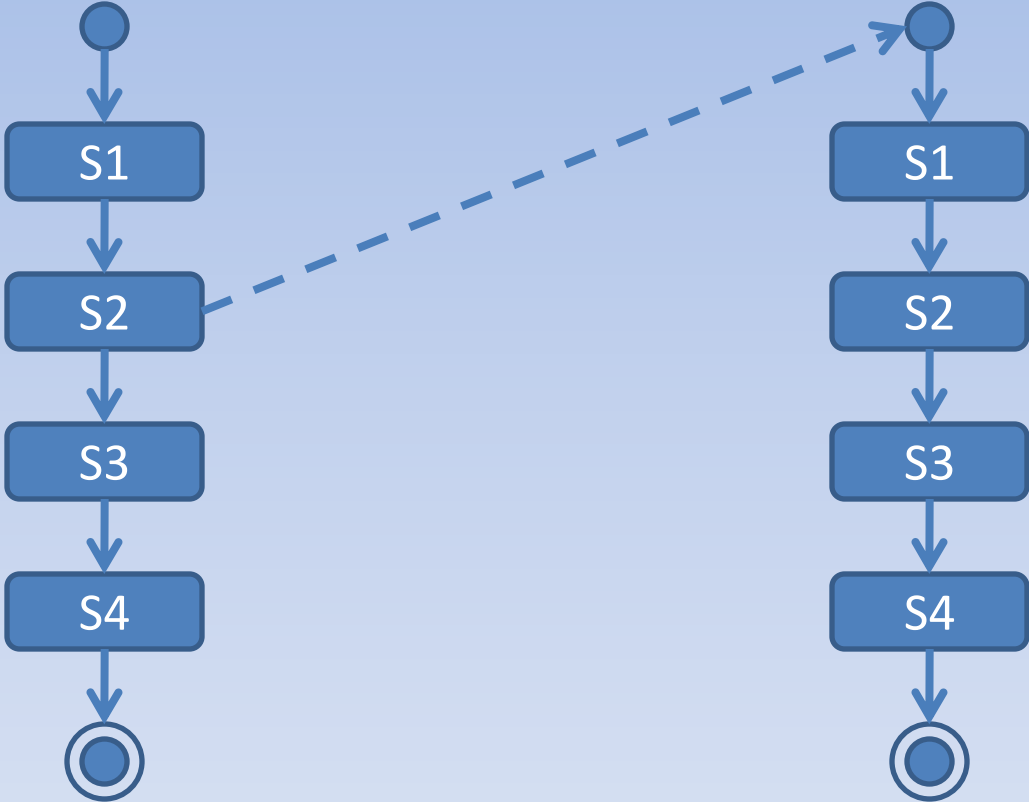
反模式



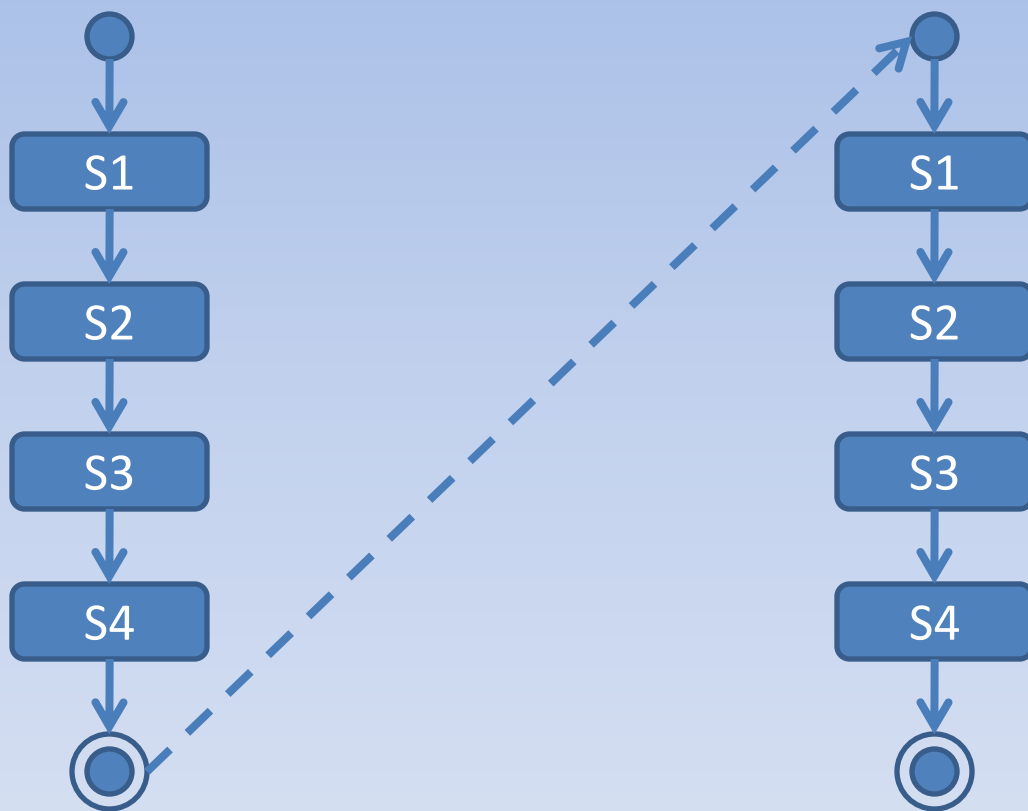
总督有自己的DSL，并可使用任何编程语言



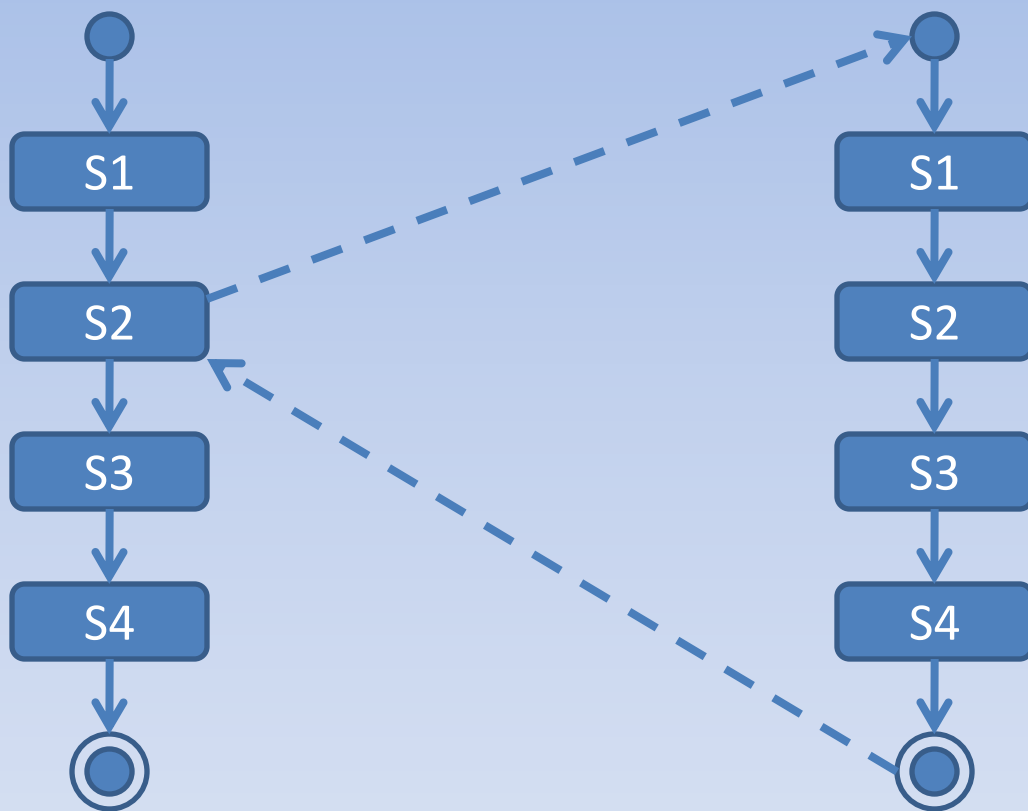
总督状态机协作关系：父子模式



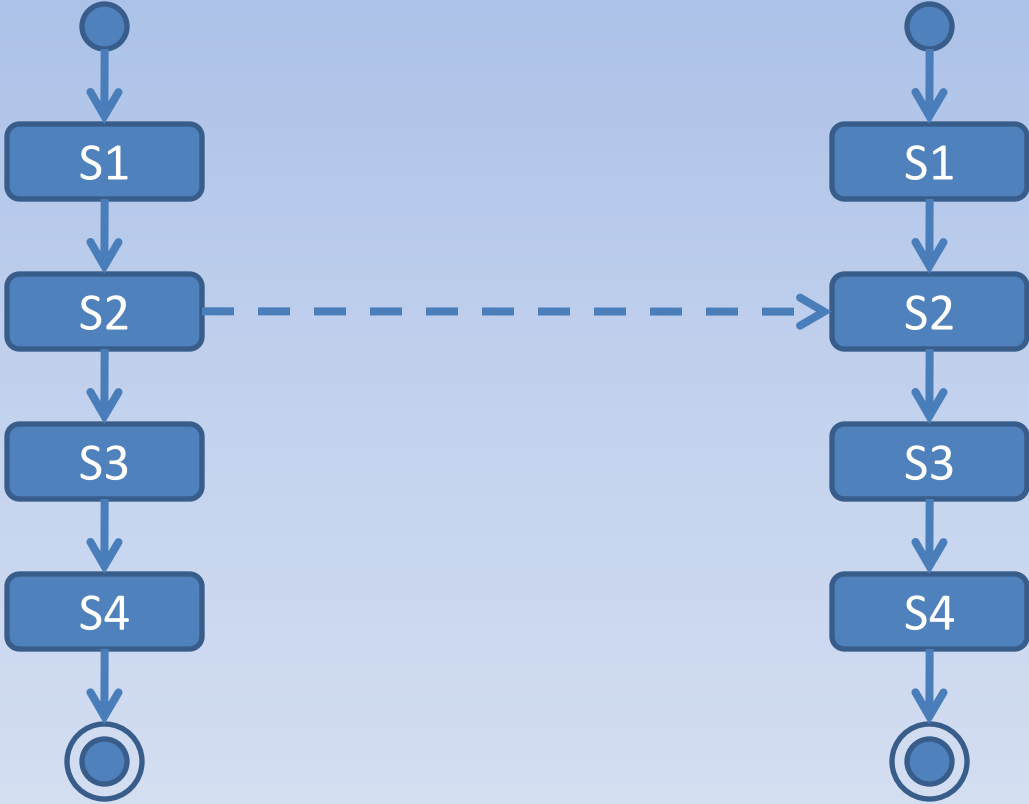
总督状态机协作关系：瀑布模式



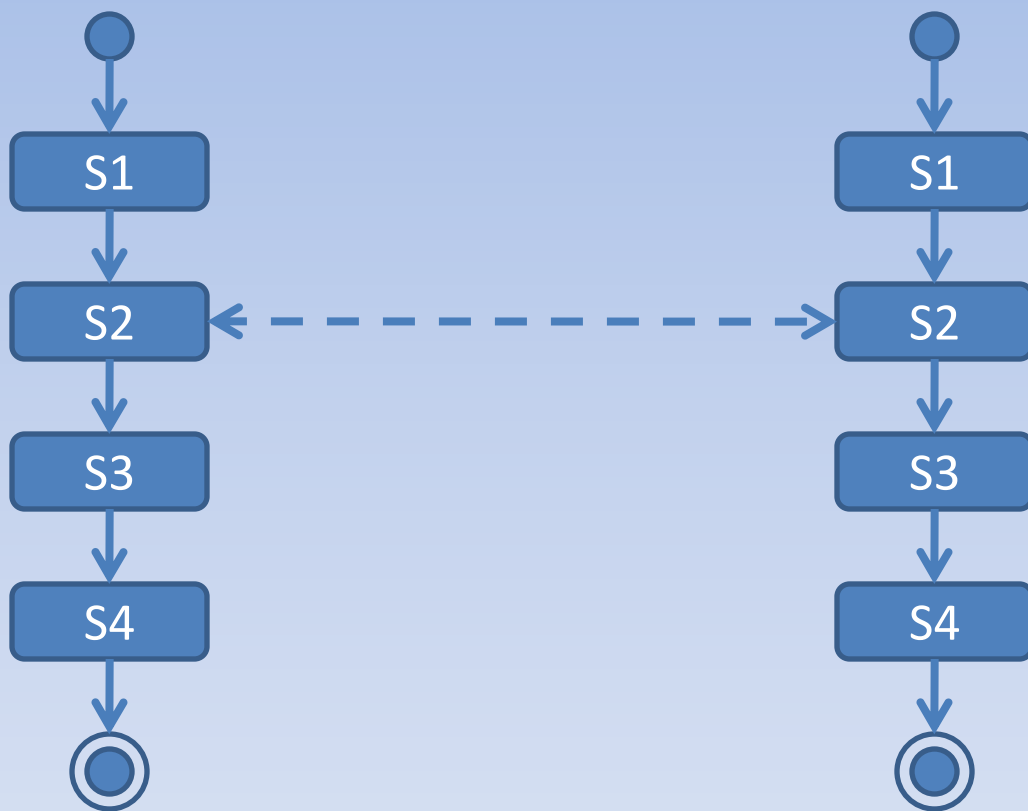
总督状态机协作关系：嵌套模式



总督状态机协作关系：通知模式



总督状态机协作关系：同步模式



CEP系统的三大难题

海量事件，处理压力太大



返乡人口众多，
请耐心等待！

网络或系统延迟，事件乱序

遵守交通次序，
请勿超车！



存在误报警的可能



小心误触警铃，
严格求证真相！

CEP的未来令人期待...

2010年的CEP



A full-body image of Superman standing against a blue sky with white clouds. He is wearing his iconic blue suit with a red and yellow 'S' shield on his chest, a yellow belt, and a large red cape that is blowing in the wind. He has a serious expression and is looking slightly to the right.

若干年后…

GOOD
BYE

Created by 蔡学镛
Copyright © 2010 Alipay.com. All Rights Reserved.