第七届

数据技术嘉年华

Data Technology Carnival

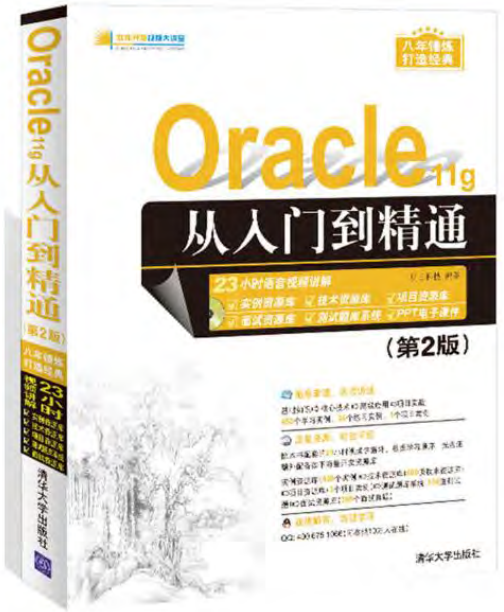
云·数据·智能 - 数聚价值智胜未来

关注公众号回复help,
可获取更多经典学习
资料和文档，电子书

大型数据中心数据安全管控

云南电网有限责任公司信息中心　　彭晓平

题外话

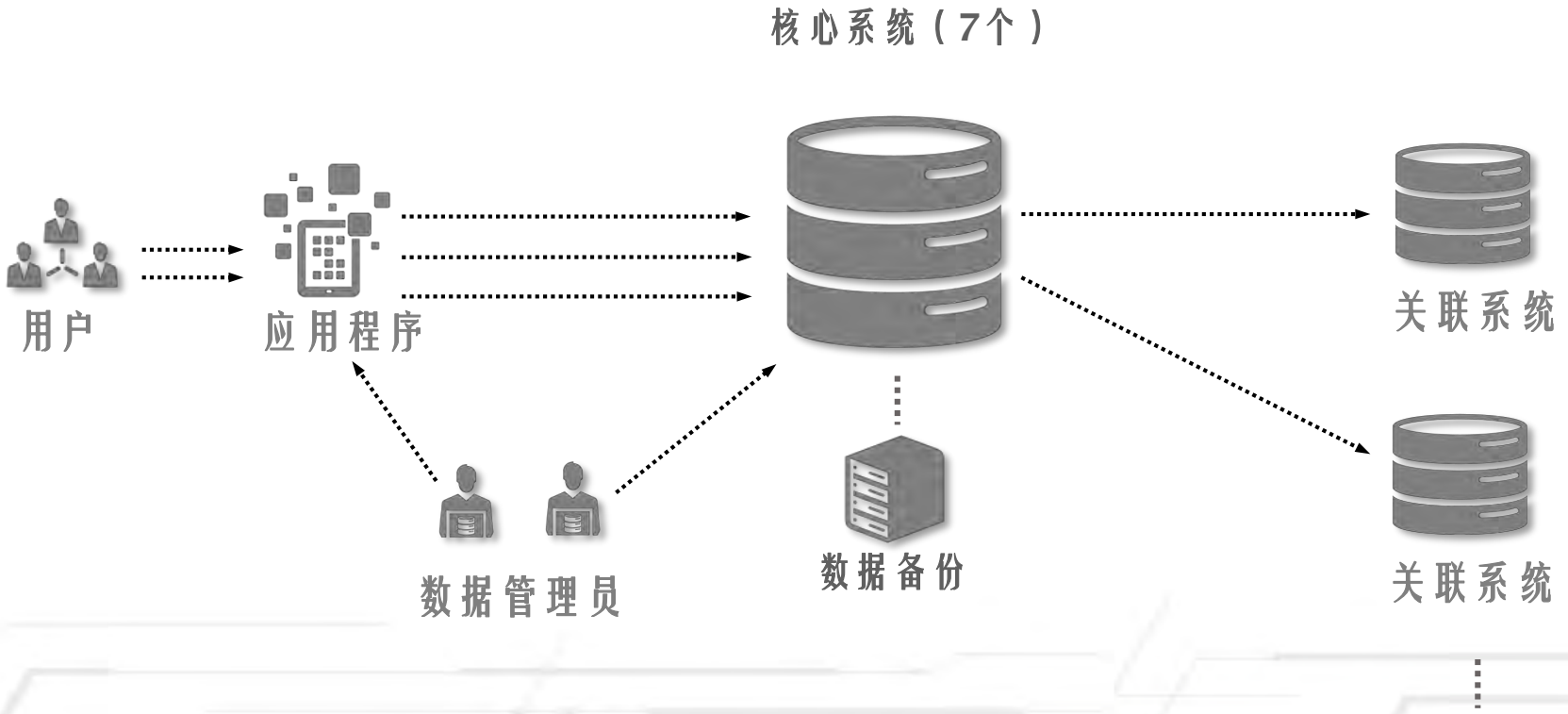


违规的操作往往带来严重的后果。作为能源行业，数据是我们的重要资产数据安全是我们的**底线**，杜绝数据泄露及不安全操作。

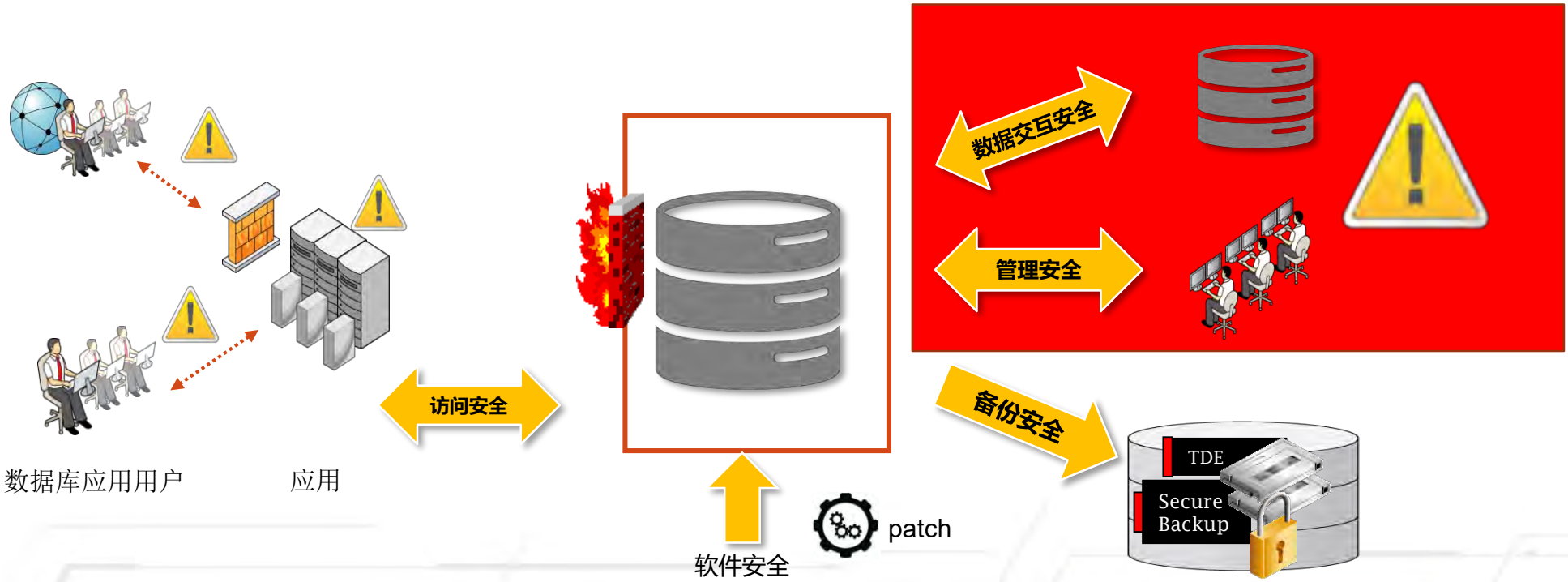
- 我们面临的问题
- 核心系统数据流向管控
- 数据运维工作管控

我们面临的问题

数据库的运行生态



数据库的安全生态

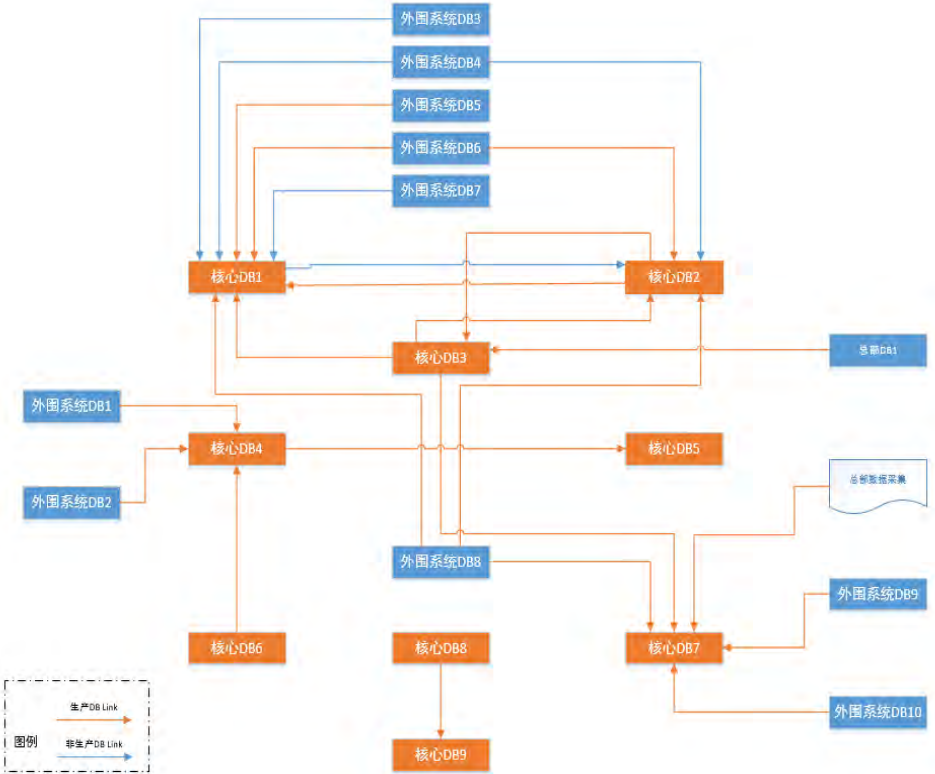

数据交互安全
管理安全
访问安全
备份安全
TDE
Secure Backup
patch
软件安全
数据库应用用户
应用

复杂的DB LINK 一

- 核心系统之间的DB Link

- 核心系统至外围系统的DB Link
  - 业务关联建立的DB Link（生产类型）
  - 非业务关联建立的DB Link（非生产类型）

- 部分DB Link用途、数据范围、交互频率不明



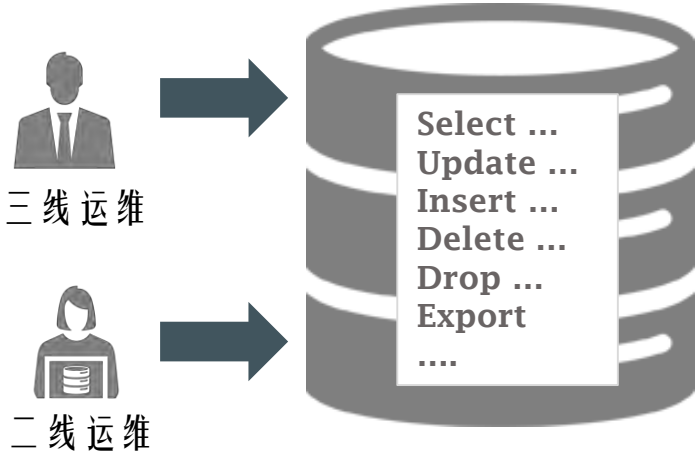
复杂的DB LINK 二

- 外围系统至核心系统的DB Link难以统计、管理
  - 外围 -> 核心系统 = 数据多副本
  - 外围 -> 核心系统(数据请求） = 性能、稳定
  - DB Link -> 核心系统(合法性） = 数据泄露
  - DB Link -> BUG = 稳定隐患

- 业务需求的变化，DB Link将变得越来越复杂，数据流向将很难梳理

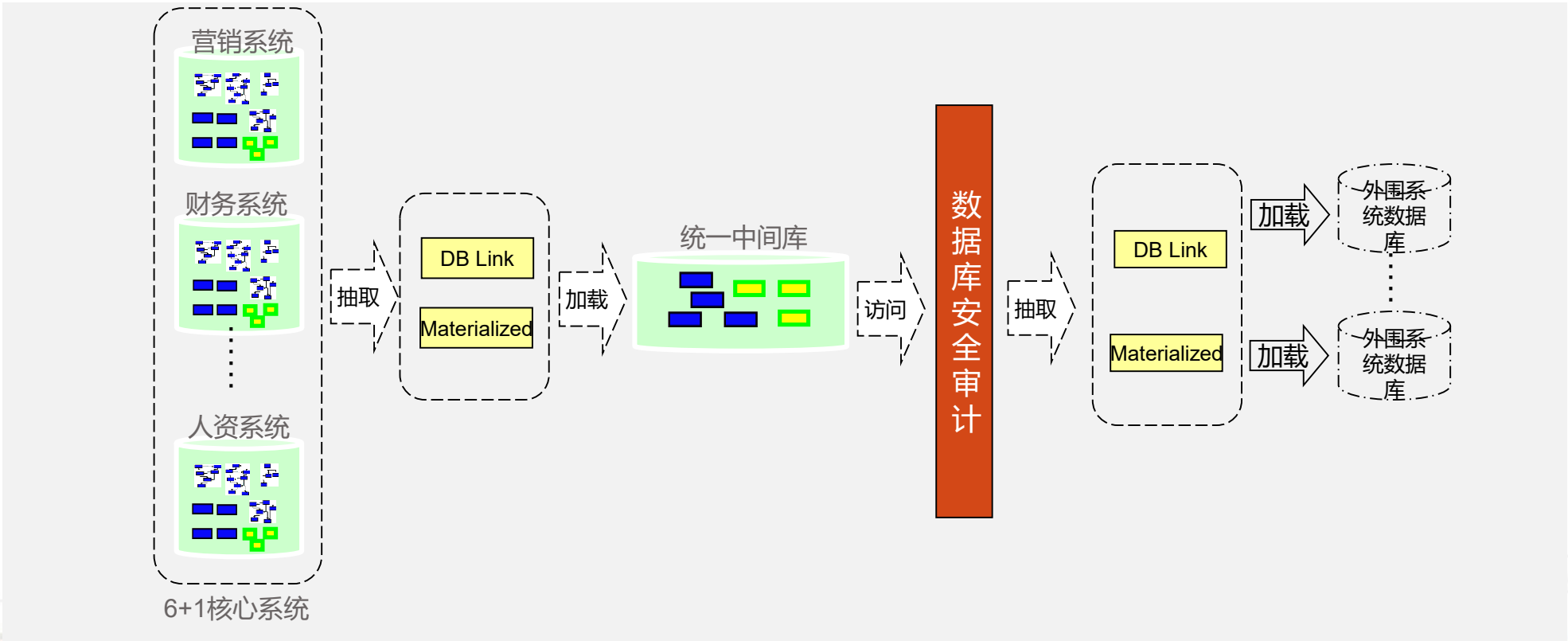
高风险的数据运维操作

- 二线运维查询、小范围修改权限
  - 查询缺乏审计
  - 通过工具查询到的数据可以直接导出
- 三线运维批量更新、DML等
  - DML操作存在误操作的风险
  - 对误操作缺乏高效的恢复手段
  - 高风险的DML操作缺乏完整的审批流程
- 二、三线运维厂家及人员较多，难以管控



核心系统数据流向管控

外围系统DB LINK隔离



外围系统DB LINK隔离策略

- 核心及外围的隔离

根据数据范围、抽取时间、抽取频率、用途，统一编排活动

- 容量、安全、数据副本最小化，按需抽取，定期清理
- 细粒度的审计，流向、事件可追溯、问责
- 逻辑同步方式，适合于对数据实时性要求不高的连接场景

中间库设计

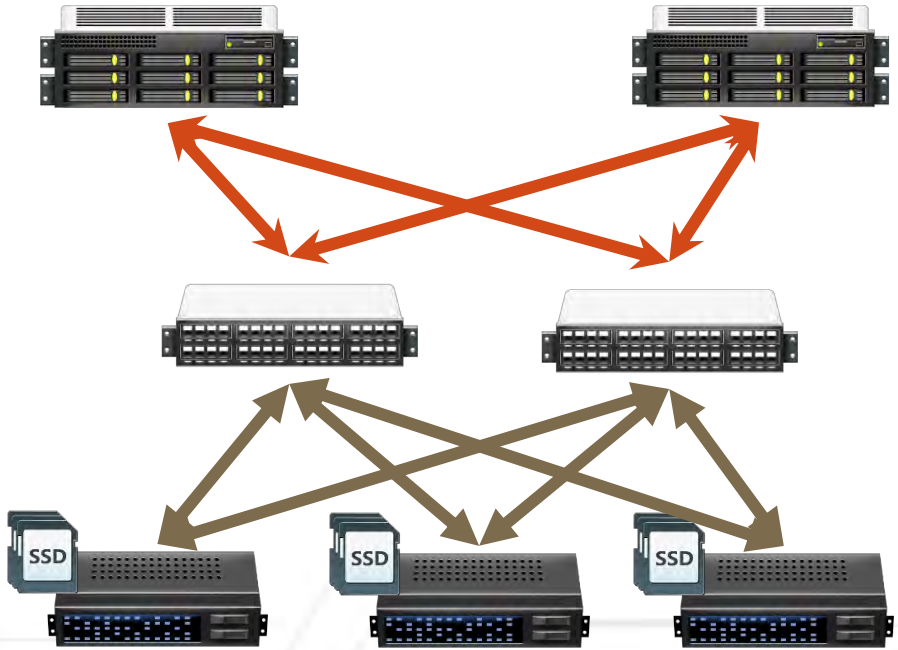
- 中间库也成为了准核心系统

外部业务持续提供，必须具备**高可用**性

- 采用两节点的RAC架构
- 网卡、交换机等基础设备都配置冗余
- 利用ASM对数据进行冗余

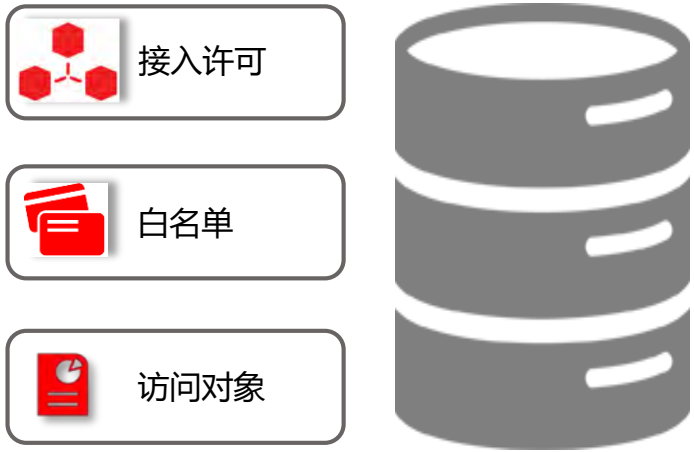
负责对外连接，需具备**高性能**

- 采用分布式存储
- 采用Infiniband交换机
- 按3个存储节点测试，IOPS 100W+，Latency < 0.6 ms，MBPS 17GB/s



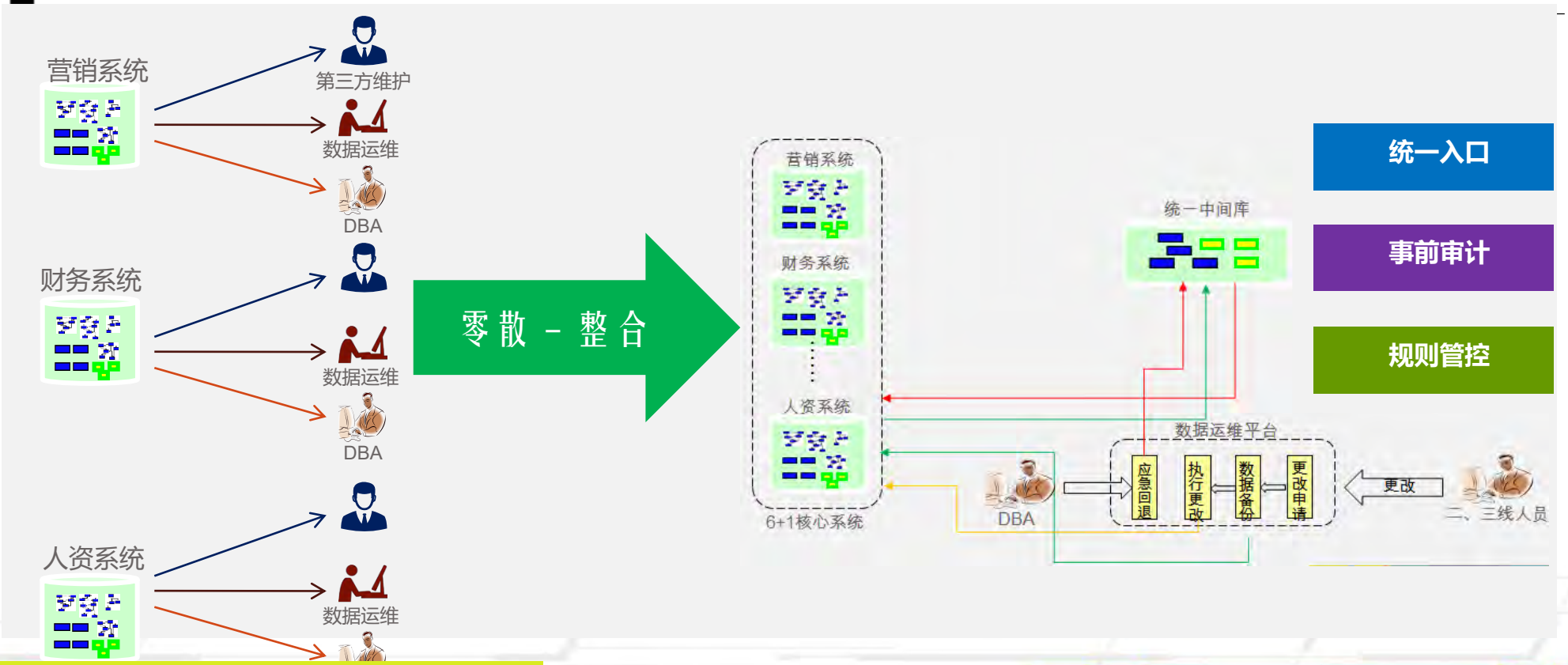
最佳实践

- 严格控制接入
  - 需要有业务部门审批
  - 有生命周期管控
- 数据库白名单定期清理
  - 分析连接情况，三个月未发生数据库访问源IP，考虑清理
- 基于访问对象的管控
  - 按访问对象进行管控
  - 一连接，一账号



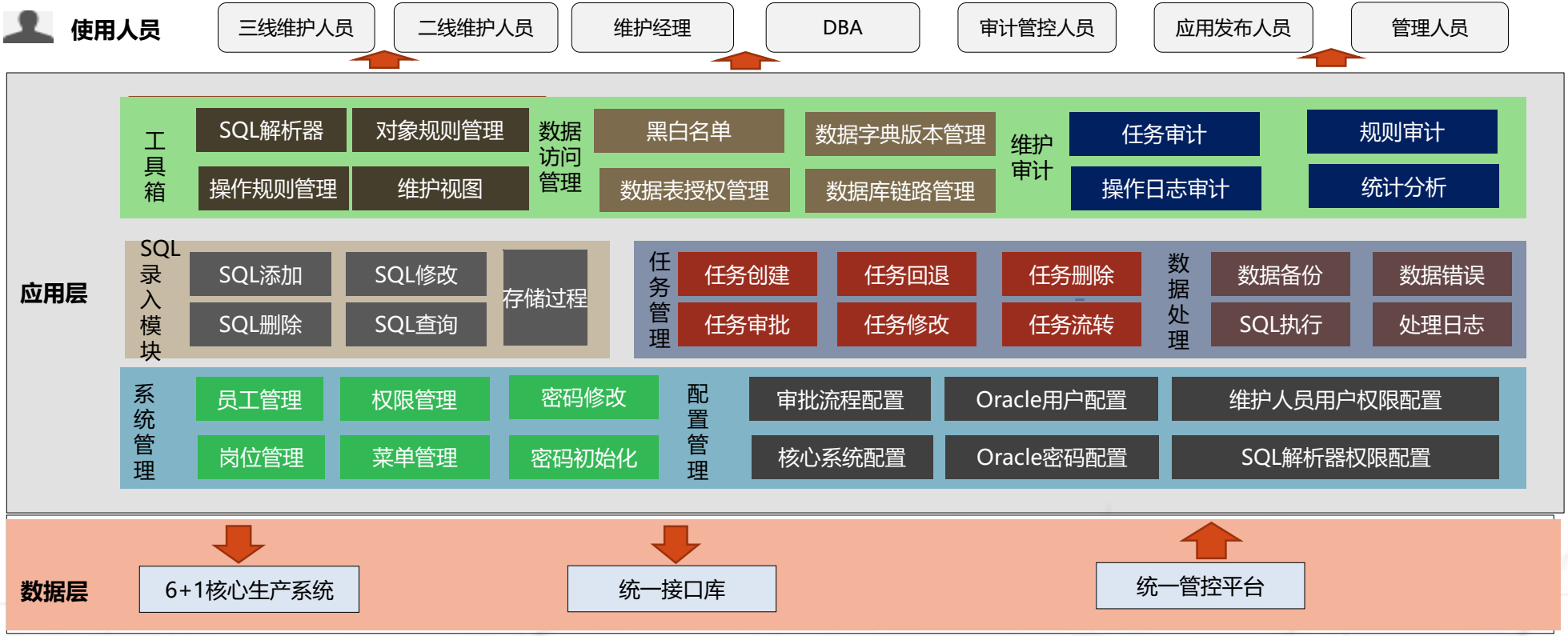
数据运维工作管控

数据运维工作管控

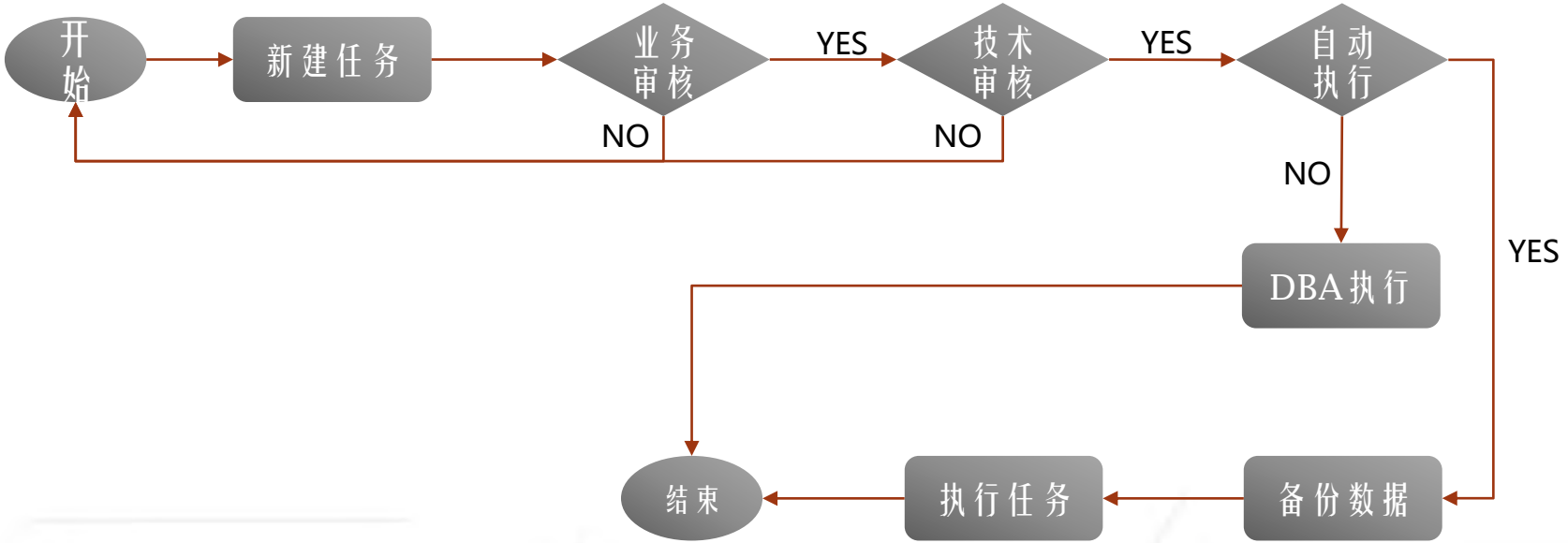


PL/SQL Developer、SQL*Plus、TOAD、OEM等管理工具

数据运维平台架构


使用人员
三线维护人员
二线维护人员
维护经理
DBA
审计管控人员
应用发布人员
管理人员
应用层
工具箱
SQL解析器
对象规则管理
操作规则管理
维护视图
数据访问管理
黑白名单
数据字典版本管理
数据表授权管理
数据库链路管理
维护审计
任务审计
规则审计
操作日志审计
统计分析
SQL录入模块
SQL添加
SQL修改
SQL删除
SQL查询
存储过程
任务管理
任务创建
任务回退
任务删除
任务审批
任务修改
任务流转
数据处理
数据备份
数据错误
SQL执行
处理日志
系统管理
员工管理
权限管理
密码修改
岗位管理
菜单管理
密码初始化
配置管理
审批流程配置
Oracle用户配置
维护人员用户权限配置
核心系统配置
Oracle密码配置
SQL解析器权限配置
数据层
6+1核心生产系统
统一接口库
统一管控平台

DML/DDL审核流程



工具箱-常用查询

二线运维人员提出查询需求

业务审核需求的合理性

DBA业务专家编写查询语句

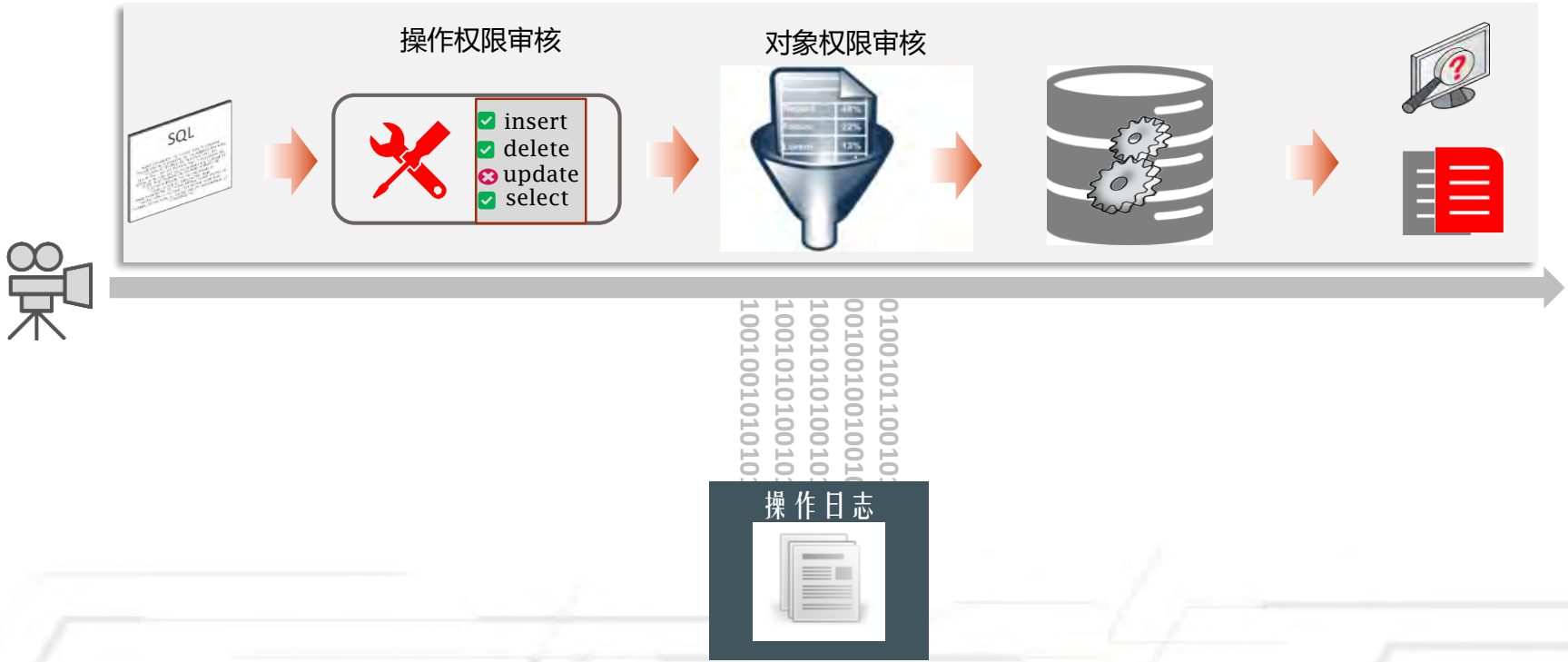
DBA录入SQL语句

DBA或厂家测试SQL语句

发布

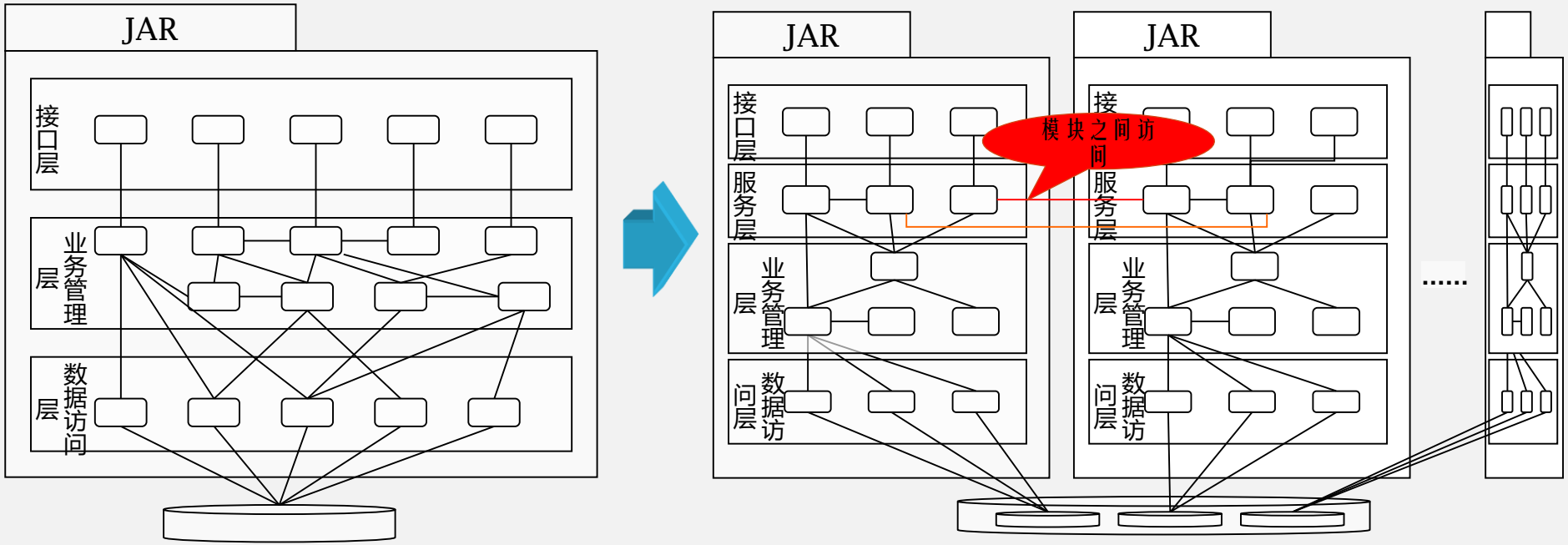
运维人员

SQL解析器

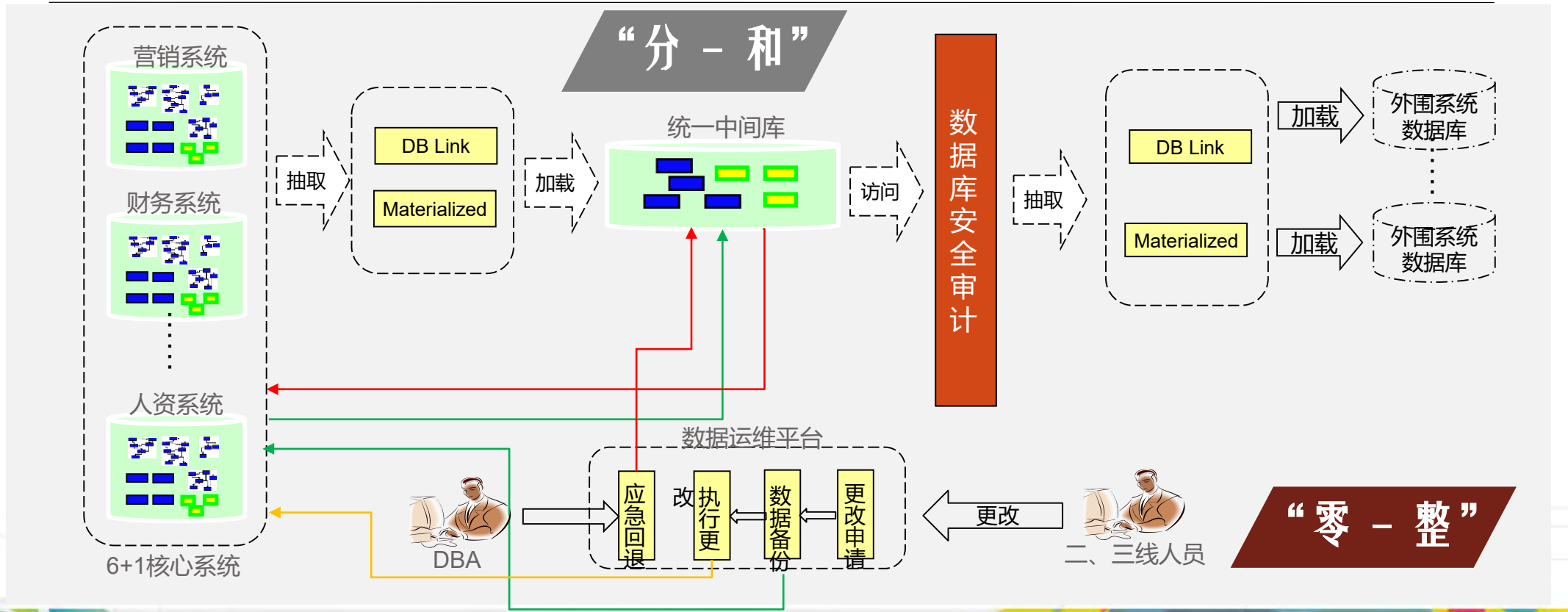


数据运维平台架构设计

划分功能域 | 分JAR设计 | 对外接口 | 内部服务编排 | 外部集成服务



核心数据安全接入层全景图



安全管控成效

- **数据流向重定义**
- -实现数据聚合、分发，提升生产库的安全稳定性。
- **数据运维统一入口**
- - 去除直连，所有数据更新通过平台展开。二线、三线统一标准，提升接入安全。
- **事前审批+事后审计：**
- - 数据变更操作必须经过审批后才能执行。
- - 对数库的任何操作都有操作记录日志，事后可审计，可追溯。
- **自动备份+快速恢复：**
- - 基于录入的SQL执行自动解析、备份语句重组、自动数据备份。
- - 误操作可以快速回退。
- **数据服务定制化：**
- - 提供工具箱，实现数据维护工作快捷化，定制化。

一个分享交流的地方

微信号：eyygle

Long Press QR Code To
Identify The Concern

长按二维码识别关注

扫一扫，加入我们，分享更多知识

THANKS