



Agent运维的落地探索与风险管控

陕西农信 科技部 党勇

一、

运维工具建设历程

二、

运维工具体体系建设痛点

三、

AI时代下的运维思考

四、

分阶段建设规划

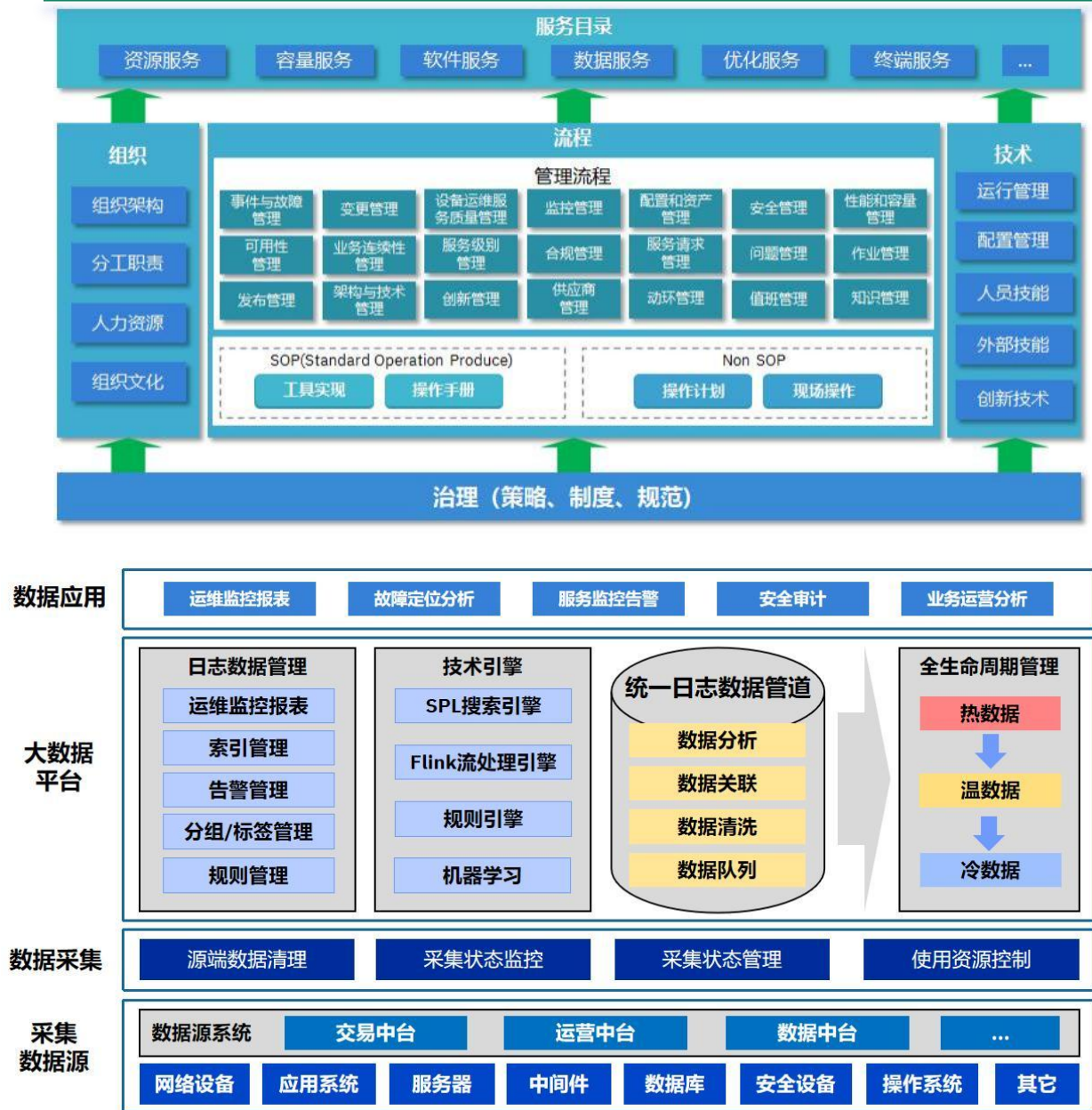
五、

AI风险与控制

六、

未来展望

一、运维工具建设历程



研发技术引入



163项目群

互联网金融平台
信贷管理平台
客户信息管理平台



微服务、云容器化
全行级微服务框架
分布式技术平台



应用单元化
新一代核心系统
项目群投产

运维工具建设

2014

第一代IT综合监控平台

2016

工具能力补齐

应用性能监控平台
IT运维服务流程系统
日志管理平台
自动化运维平台
配置管理平台

2021

分布式服务监控系统

调用链监控系统
运维数据中台
运维数据分析系统

2025

智能化建设

新一代智能化监控平台

2026

.....

二、运维工具体体系建设痛点

01



运维投入有限

- 数字化转型及国产化改造，环境变动频繁，工具适配压力持续加大
- 现有监控运维工具能力捉襟见肘，逐步难以匹配业务诉求
- 运维工具零散建设，未形成一体化、体系化能力底座
- 人力、预算资源有限，难以同步落地全栈可观测等新技术建设

02



工具使用门槛高

- 各类工具专业性强，上手门槛较高，使用效果高度依赖运维人员个人经验
- 故障排查存在割裂化现象，各岗位、各工具分段处置，缺乏协同联动
- 多工具数据未打通，难以围绕同一故障形成联合分析支撑

03



工具分散割裂

- 设备、网络、应用类运维工具独立建设，以单点问题处置为核心目标
- 各类运维数据标准不统一，数据缺乏一致性与关联能力
- 跨域数据无法协同支撑统一运维目标，难以开展全局分析

三、AI时代下的运维思考

目标建立: AI赋能四大智能运维场景



从人找问题到AI找问题,构建完善的运维信息化体系

四、建设阶段一：数据AI化

智能运维场景建设

标准化

运维数据全面AI化建设

关系打通

面向AI的数据中台数据治理

CMDB建模

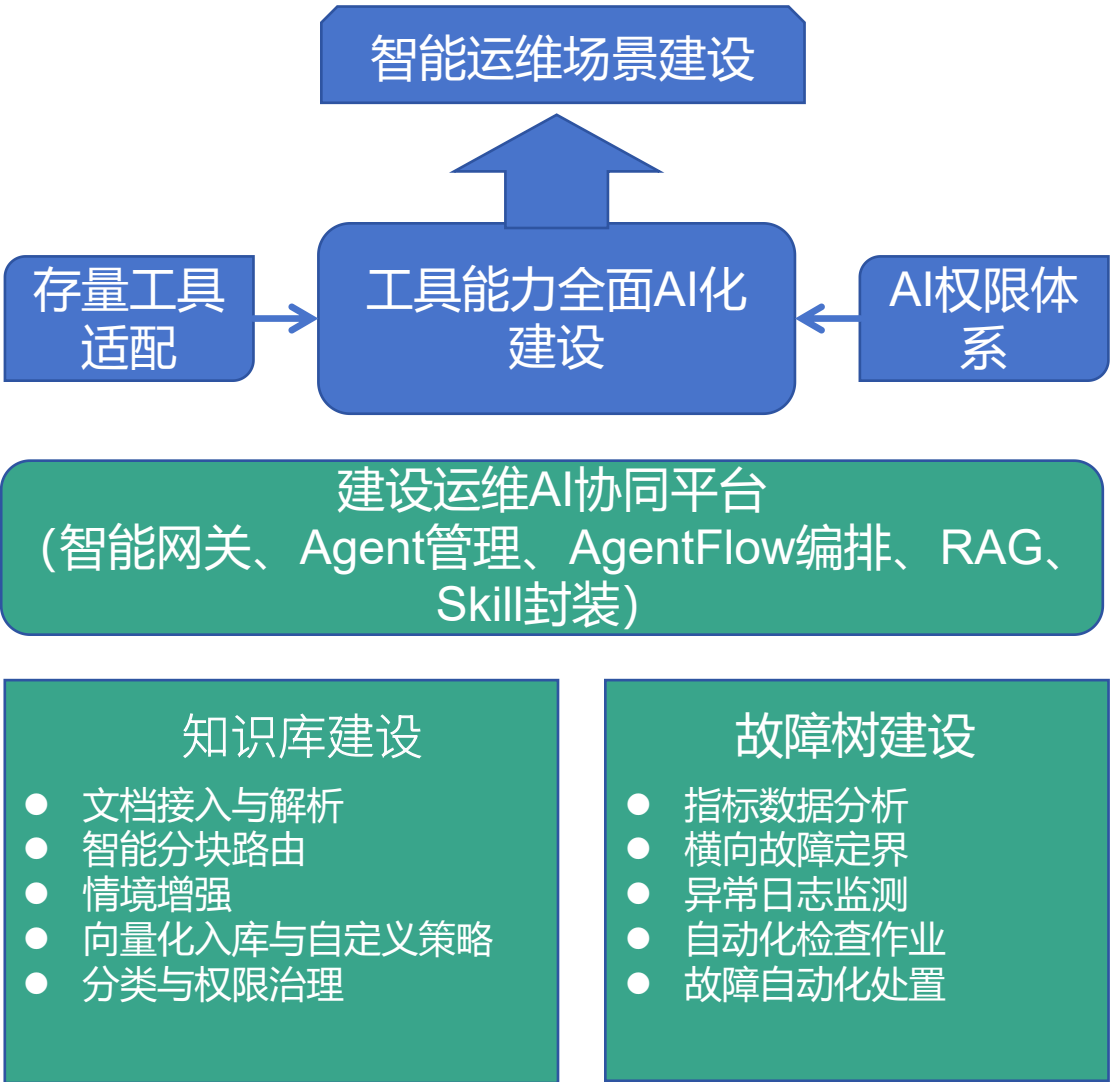
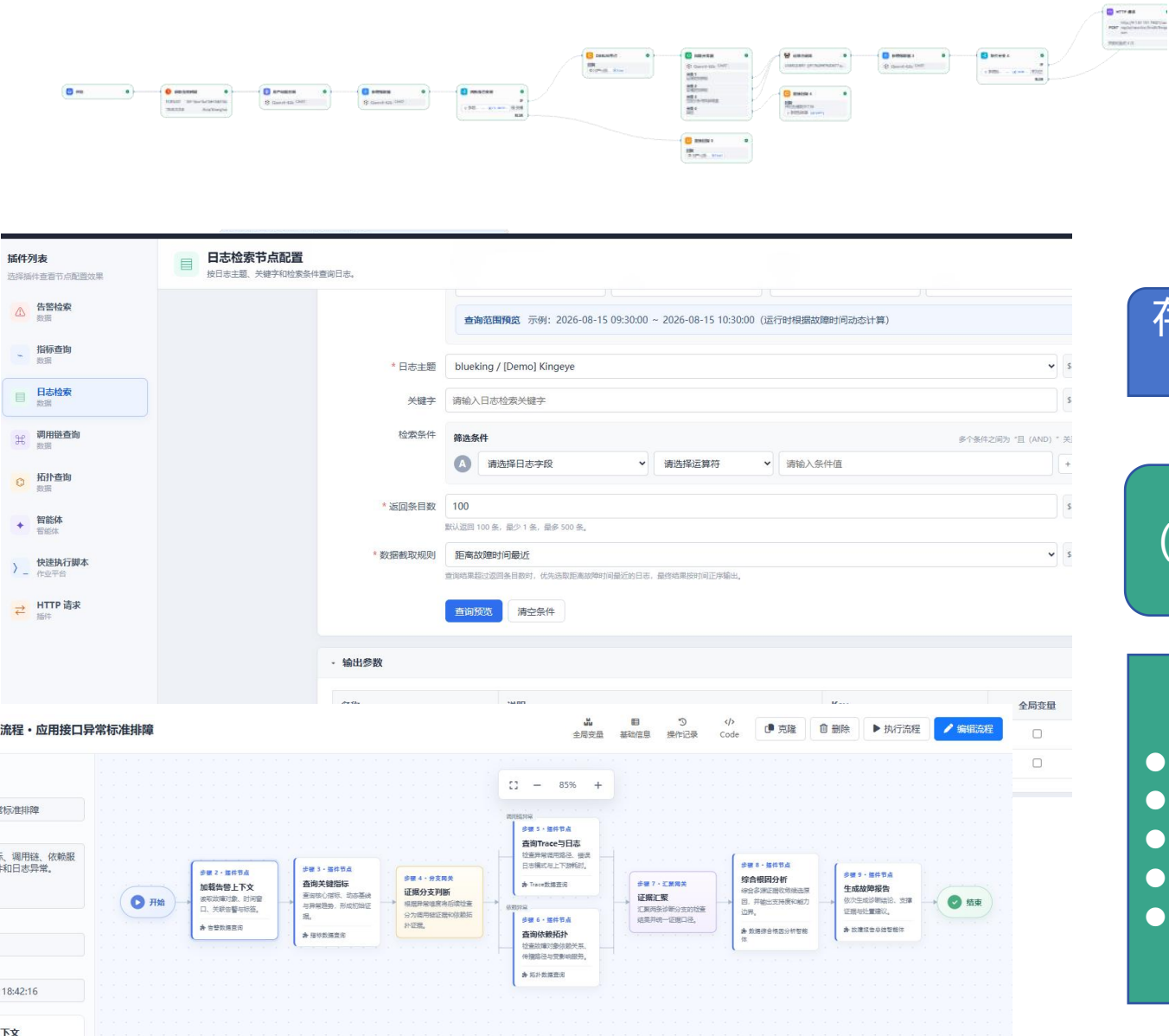
- 统一可观测口径
- 支撑故障影响分析
- 确定接入边界
- 六层对象模型
- 属性最小化原则
- 标准通用字段

数据准确性保障

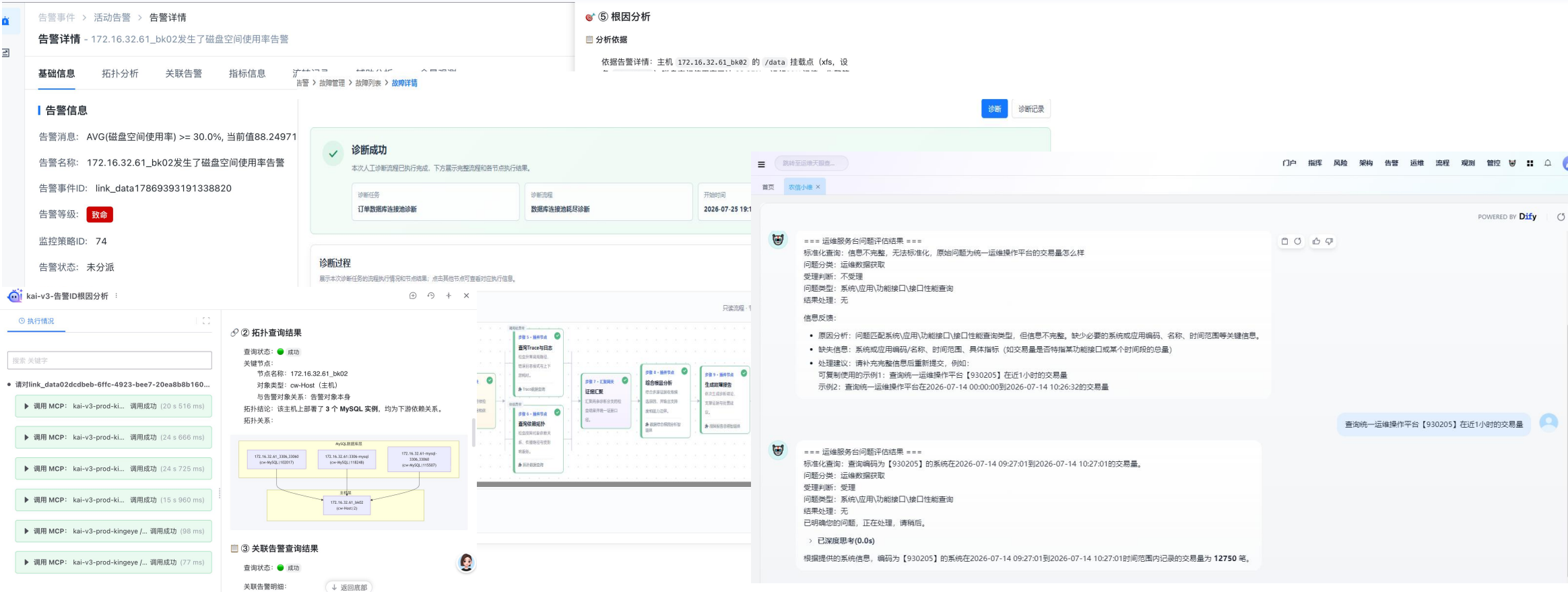
- 对象发现方案
- 关系发现方案
- 多源关系补充
- 多方核对机制
- 配置数据的全面应用
- 管理数据维护场景建设



四、建设阶段二：工具AI化



四、建设阶段三：智能场景实现



告警聚合

根因定位

AI运维服务台

数字分身

.....

落地阶段

探索阶段

规划阶段

运维数据全面AI化建设

工具能力全面AI化建设

五、AI风险与控制

数据越权风险

API网关封装+细粒度权限控制

操作越权风险

操作白名单+人工审批机制

误判风险

人工复核+置信度阈值+持续训练

数据泄露风险

数据脱敏+访问审计+加密传输

六、未来展望

现在

-  人运维机器
运维人员直接操作设备、排查故障
-  一个团队解决一个故障
多人协作、逐级排查、耗时较长
-  经验驱动、被动响应
依赖个人经验，故障发生后才介入
-  操作者角色
手动执行、重复性工作占比高

未来

-  智能体运维机器
AI智能体自主巡检、诊断、修复
-  一个人指挥一个智能体团队
单人调度多个专业智能体协同作战
-  数据驱动、主动预防
预测性维护，故障发生前主动干预
-  指挥官角色
从执行者转变为决策者和监督者

未来人在运维中的核心角色

审核

审核智能体决策
确保操作合规安全
把控关键风险节点

确认

确认运维方案
最终拍板决策
对结果负责把关

总结

总结运维经验
提炼最佳实践
形成知识资产

归纳

归纳故障规律
完善故障树体系
驱动持续优化



感谢聆听，欢迎交流