四维图语 GraphTalking

科研院所重点实验室智慧管控解决方案白皮书

适配部委/中科院科研院所，实现课题隔离、贵重科研资产追溯、全操作审计、内网安全管控

版本：V1.0（深度完整版）

出品：四维图语 GraphTalking
官网：https://www.graphtalking.com

摘要

本方案面向科研院所科研管理处、重点实验室平台负责人、课题组长、安全主管、保密管理员，解决流动科研人员权限管控难、贵重科研样品/特种试剂追溯缺失、科研数据按课题隔离、审计日志防篡改、内网保密、信创合规等痛点。基于 GT 底座，融合物资全生命周期管控、课题级权限隔离、ELN 受控电子实验记录、物联网环境监测、安全巡检、AI 安防；主打内网私有化、信创适配、全链路不可篡改审计，适配国家级重点实验室、前沿材料、能源、化学课题组等涉密/高敏感科研场景。

一、行业现状与核心痛点

1. 显性痛点

课题组人员轮换频繁：博士后、访问学者、项目聘用人员短期进出，账号开通、回收不及时；

靶材、同位素试剂、稀有标样、特种耗材价值高昂，纸质登记容易丢失、去向无法追溯；

实验记录散落在研究员个人电脑，Word、Excel 版本混乱，结题溯源、成果复盘困难；

主管部委安全检查、保密审计，需要调取每一步操作记录，人工整理审计材料工作量极大；

精密实验对环境（气体、压力、温湿度）敏感，环境超标缺少联动告警。

2. 隐性风险

越权访问风险：不同课题数据混杂，A 课题人员查看 B 课题敏感数据；

审计失效风险：日志可删除、可修改，审计证据不被主管部门采信；

数据外泄风险：公有云 SaaS 方案数据出内网，不符合院所保密管理规定；

资产流失风险：高价值科研物资缺少闭环管控，流失后无法定位责任人。

二、政策合规依据

《危险化学品安全管理条例》

科研设施与仪器开放共享管理办法

科研数据管理相关规范

科研单位保密管理规定

信创产业相关采购要求

三、建设思路与总体架构

建设思路：保密优先、课题隔离、全程可审计、贵重科研资产闭环管控、科研记录规范化、内网封闭运行。

【图注占位】

图 1 GT 科研管控总体架构图（含审计引擎、物联网网关、课题权限引擎、ELN 记录系统、物资管控、AI 安防）

底座内置不可篡改审计日志引擎；感知层包括气体、压力、温湿度传感器、门禁、摄像头（选配）；业务层覆盖课题权限管理、贵重物资一物一码流转、受控 ELN、安全巡检、仪器机时统计、环境联动告警；部署边界默认内网私有化，禁止公网传输科研业务数据；对接院所统一身份、科研项目管理系统。

四、核心业务模块详解

1. 精细化课题权限引擎

区别于传统按部门划分权限，支持课题维度独立数据域隔离。同一平台内，课题组人员仅能查看本组样品、实验记录、仪器使用数据；平台管理员拥有跨课题审计权限；支持临时账号、账号有效期自动过期，项目结题自动回收权限。

2. 贵重科研物资全生命周期管理

靶材、特种试剂、稀有样品、同位素物料扫码管理：入库、领用、转移、归还、外送测试、灭活销毁全部交接留痕；高价值物料流转可设置多级审批。

3. 受控 ELN 电子实验记录本

记录绑定课题、样品、仪器；版本锁定，修改自动生成修订痕迹，记录修改人、修改时间、前后版本；支持 SOP 集中归档，满足项目结题、科研成果溯源要求；记录归档后禁止随意删除。

4. 全链路审计日志引擎

登录、查看记录、导出、修改、物资领用、权限变更全部写入审计库；日志不可删除、不可篡改；支持按人员、课题、时间段筛选，一键导出审计包用于保密、安全审计。

5. 物联网环境监测联动模块

实时采集实验室内压力、可燃/有毒气体、温湿度；阈值自定义，超限推送告警，支持联动排风、声光报警，保护精密实验条件。

6. 仪器机时统计与课题费用分摊

大型共享仪器预约、机时统计，按课题归集使用时长，支撑平台绩效考核、科研经费分摊核算。

7. AI 视频安防、安全巡检（选配）

实验室违规识别、巡检工单闭环，和物资台账联动。

五、差异化优势对比

维度	普通 LIMS	公有云平台	普通安防	四维图语
课题级软隔离	✘ 多为部门权限	✘	✘	原生支持
数据出内网	—	上公网	—	✘ 完全不出网
审计日志防篡改	弱	—	无	不可篡改
科研物资/ELN 体系	部分	—	无	全链路
信创私有化	部分	✘	—	全面适配

六、部署、信创与保密适配

强制私有化内网部署，数据不出院所内网；全面适配国产服务器、国产操作系统、国产数据库；可对接院内网准入体系；所有导出操作留下审计痕迹。

七、实施、培训

重点工作：前期梳理课题矩阵、人员权限模型、物资审批流程；专项培训保密管理员、平台管理员；交付审计台账使用指南；严格遵循院所内网安全规范，不引入外网通道。

八、运维与保障

内网环境专项运维方案；定期日志完整性校验；算法、系统版本升级在内网离线包交付，不依赖外网更新。

九、典型场景

国家级重点实验室、能源/材料/化学前沿课题组、同位素实验室、院所公共仪器共享平台。

十、选型避坑指南

避坑 1：不要选用公有云 SaaS 方案，直接无法满足保密内网隔离；

避坑 2：区分部门权限和课题权限，很多厂商只能做到部门隔离，做不到课题软隔离；

避坑 3：重点核验审计日志能力，确认日志是否真的不可删除，而不是普通操作记录；

避坑 4：ELN 重点看版本修订留痕、归档防删除能力，而不是简单在线填表。

十一、结语

科研院所实验室数字化的第一优先级不是迎检减负，而是守住科研资产安全、敏感数据隔离、全流程可审计，支撑主管部委安全、保密检查。如需获取演示、详细方案，请访问四维图语官网。